Alternative Desktop Computing

ThinManage 3.1

Administration Manual

Notice

Devon IT, Inc. reserves the right to revise and improve its products as it deems necessary. This manual provides a description of the product at the time of printing, and may not necessarily be accurate for future or past releases. Please visit our website to download the latest version of this document: www.devonit.com

Devon IT, Inc.
1100 First Avenue
King of Prussia, PA 19406 U.S.A.
www.devonit.com

Table of Contents

Chapter 1

Virtual Appliance Installation and Setup

Topics Covered :

- *Downloading VMware and the ThinManage Software*
- *Initial Virtual Machine Setup*
- *Step-by-Step Guide for Configuring the ThinManage Server*
- *Final Configuration*
- *Checking Connectivity*

1.0 Virtual Appliance Installation and Setup

Required components:

- One or more desktop access devices
- ThinManage virtual machine
- System running VMware Server or VMware player
- System running DNS and DHCP servers

Download and Install VMware® Server or Player

Download and Install VMware Server or VMware Player on a dedicated system:

- http://www.vmware.com/products/

If you need assistance installing VMware, please visit:

- http://www.vmware.com/support/pubs/

Download the ThinManage Software

Download the latest ThinManage software and Host Agent Setup files from Devon IT's FTP Server.

FTP Location:

Server: `ftp://mx2.devonit.com`

Username: `Images`

Password: `nt@t3rminal5`

Virtual Appliance Path: `ThinManage/v3/Appliance/ThinManage-appliance-<yyyymmdd-hhmm>.zip`

Host Agent Path: `ThinManage/v3/Host-Agent/AgentSetup.exe`

The ThinManage software will follow a naming convention of `ThinManage-appliance-<yyyymmdd-hhmm>.zip`, where `<yyyymmdd-hhmm>` is the build's datetime stamp.

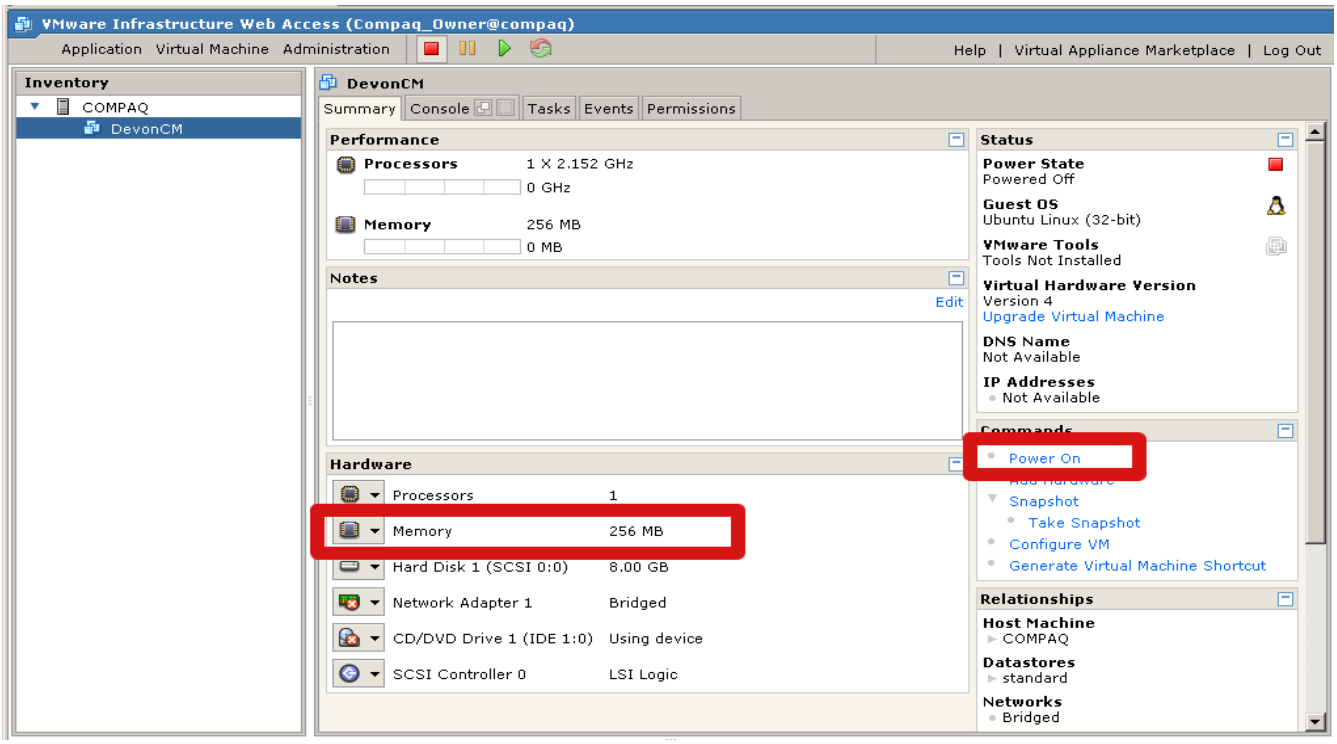
Extract the ThinManage trunk archive on the same machine that your VMware Server or Player is running on. After the extract, you should have a folder called “ThinManage” that contains the necessary VMware files (.vmdk and .vmx).

Initial Virtual Machine Setup on VMware

VMware Server 2.0

These are the steps for setting up the virtual machine on VMware Server version 2.0

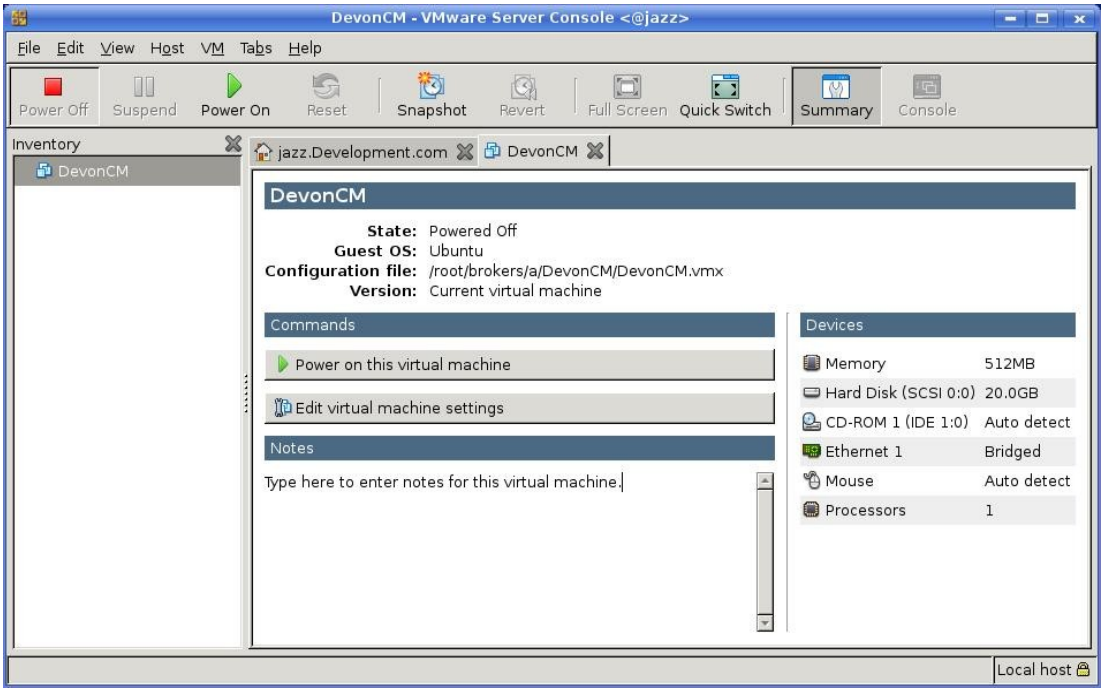
- Open your VMware Infrastructure Web Access page.
- From the top toolbar, select **`Virtual Machine -> Add Virtual Machine to Inventory`**
- Begininng with the Inventory column, use the tree-like navigational system to drilldown to your ThinManage folder until you finally reach the file called **`ThinManage.vmx`**. Then press the **OK** button



- Back on the VMware Infrastructure Web Access page, under **`Inventory`**, select **`ThinManage`**.
- Depending on the amount of memory available on your host system, you may need to adjust the allocated **`Memory`** from the default 512MB to a lower value. (See screenshot above).
- Lastly, **`Power On`** your ThinManage virtual appliance.

VMware Server 1.0.x

These are the steps for setting up the virtual machine on VMware Server versions 1.0.0 through 1.0.8

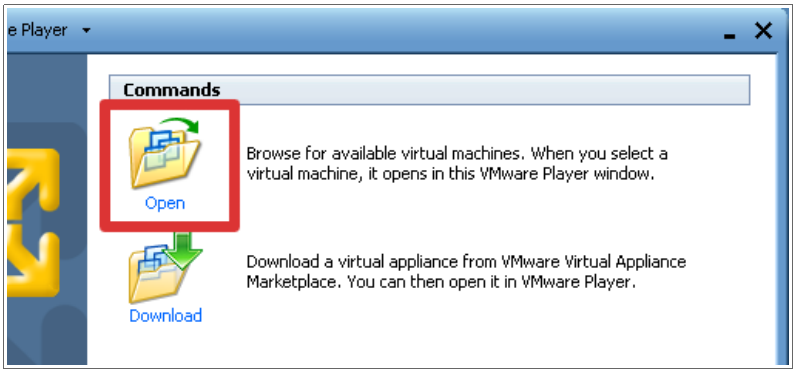


- Choose **`Open Existing Virtual Machine`**
- Choose **File → Open** and **Browse** to the **`ThinManage.vmx`** file on your machine.
- The virtual machine name is called **`ThinManage`**
- Depending on the amount of memory available on your host system, you may need to **adjust the Allocated Memory** from 512MB to a lower value.
- Click **`Start this virtual machine`**

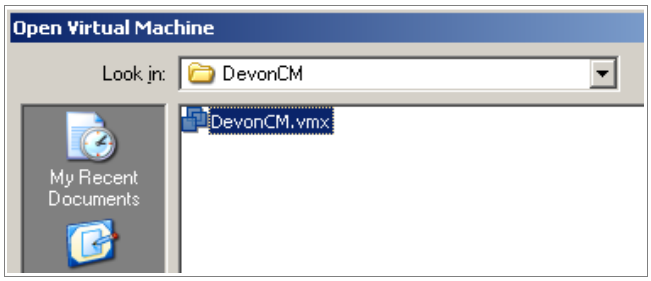
VMware Player

These are the steps for opening the ThinManage virtual machine on VMware Player.

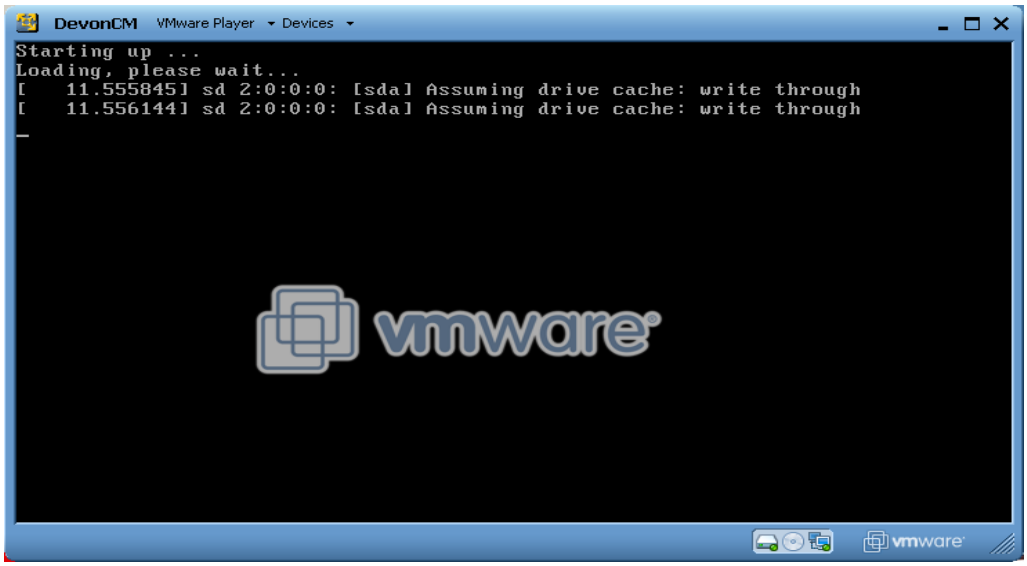
- Launch VMware Player on your system. Click the “Open” icon.



- Open the **`ThinManage.vmx`** file located in the ThinManage folder

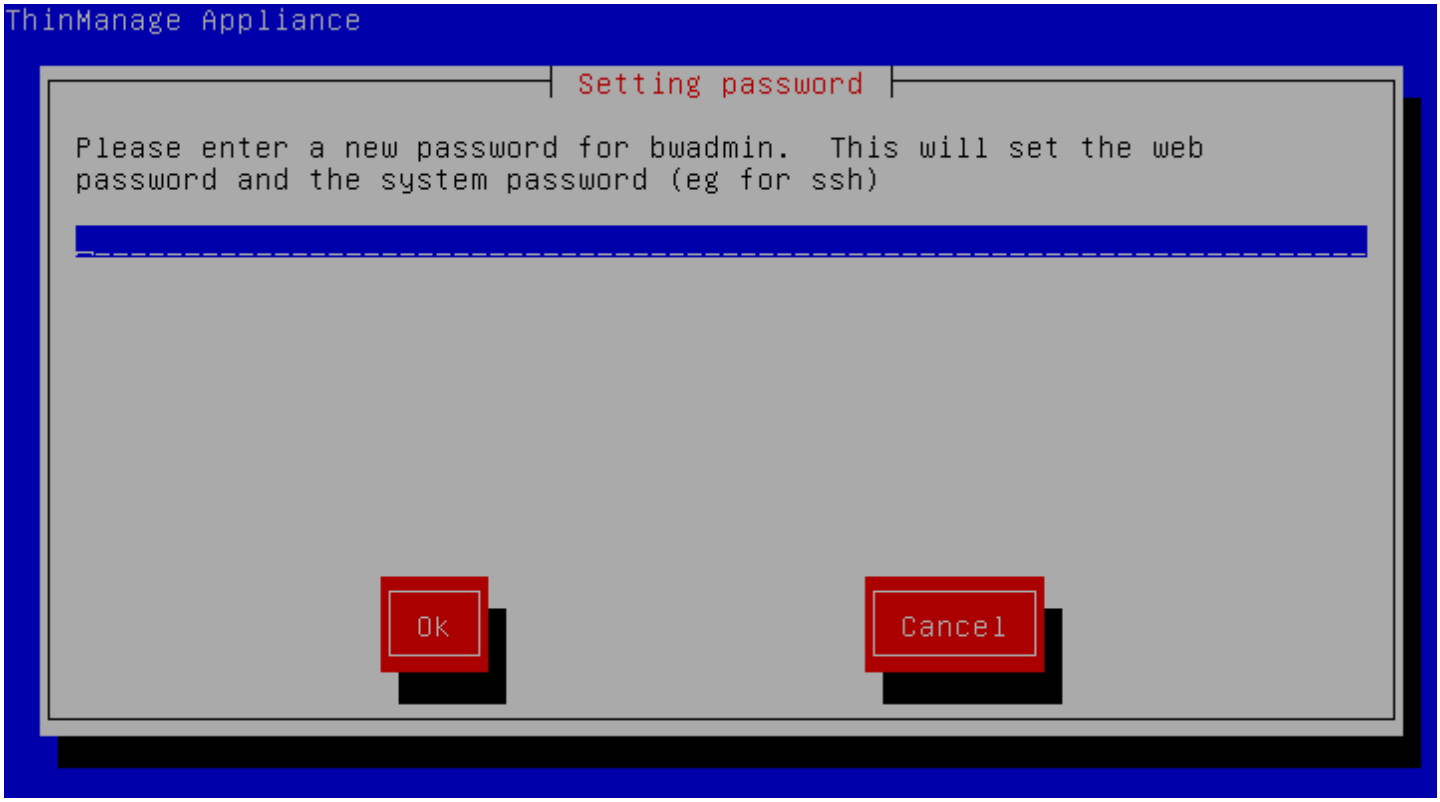


- Your virtual appliance will immediately begin booting.



ThinManage Appliance Password and Timezone Configurations

1. Turn on the Virtual Machine
2. After the bootup process is complete, you will be presented with the **Setting Password** window
3. Enter a new password for the **bwadmin** account.
4. Once a password has been entered, use the arrow keys on your keyboard to navigate to the **OK** button and press Enter to continue. You will be prompted to re-enter the password a second time. Press **OK** button again to continue.



5. The next menu allows you to set the timezone for the ThinManage appliance. Select your geographic area from the list and press Enter.

6. A list of cities will appear. Select a nearby city that is located in your time zone and press Enter.

ThinManage Network Configuration

DHCP Configuration (default)

The next screen is the **Networking** configuration menu. By default, the ThinManage Appliance will attempt to acquire an IP Address from DHCP on your LAN. The fourth option will read **"Change eth0 inet dhcp <ip-address> <subnet mask>".** If DHCP was successful, then no further configuration is required and you may select **No Changes** and press Enter to continue.

Static IP Configuration

If DHCP is not available on your LAN, then you will have to manually set a static IP address for the ThinManage server. Select option **Change eth0...** from the Networking menu.

1. On the next screen named, **Configuring eth0**, select option **Static** and press the **OK** button to continue.

2. Enter a static IP address at this time. Press OK to continue.

3. Enter the subnet mask and then press OK to continue.

4. Enter the Gateway IP address and press OK.

5. Once these three values have been entered, you will be asked to confirm the new static settings. Select **Yes** to apply the new settings. Otherwise, select **No**, to discard these changes.

6. After selecting Yes, the network interface will restart and you will be presented with the **ThinManage Appliance Main Menu.**

7. When using a static address, you need to edit the ThinManage Server's **`resolv.conf`** file. This file contains the ip address to your DNS server(s) as well as domain search paths.
   - From the Main Menu, select **`Reconfigure networking`**
   - Select **`DNS view/edit resolv.conf`**.
   - Using the editor, make sure your file contains, at a minimum, the following two lines:

     `search <domain>`

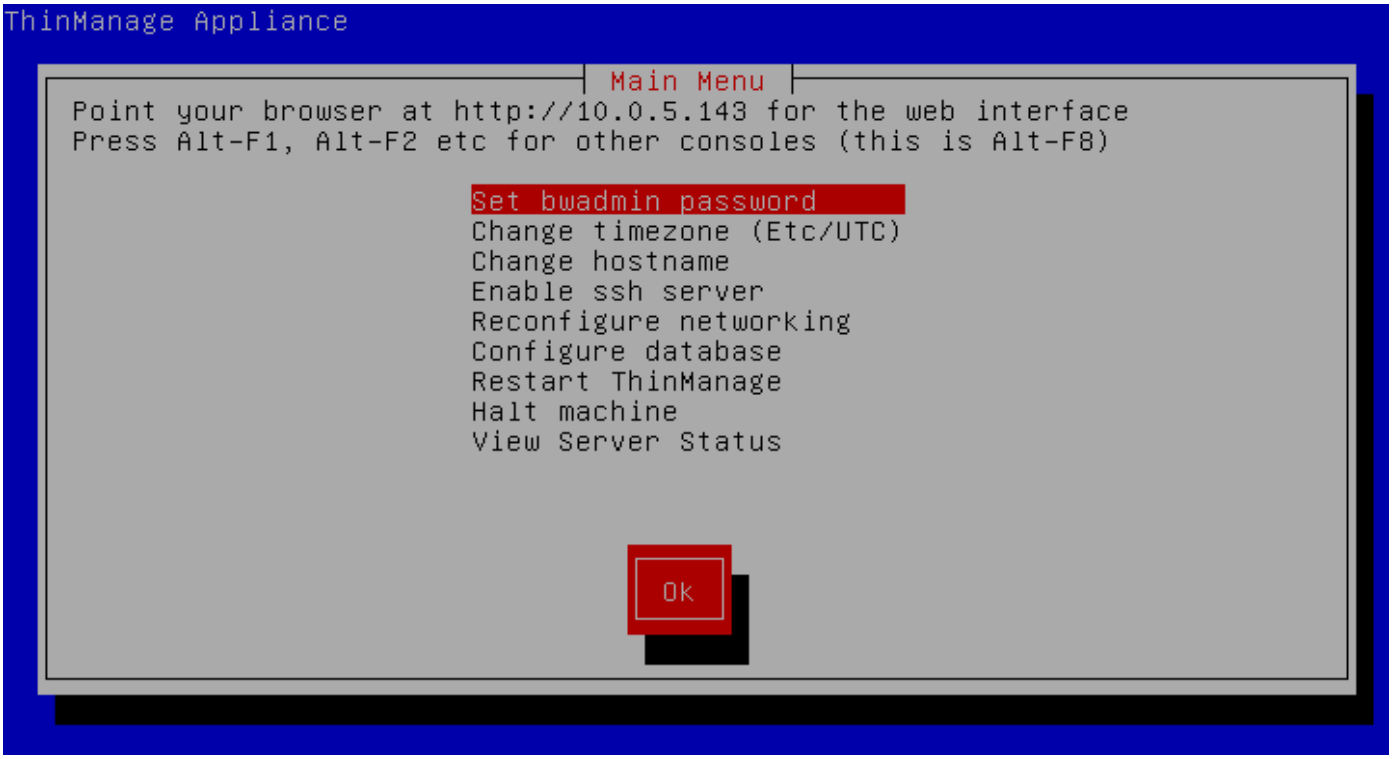
     `nameserver <ip address>`

     Where *<domain>* is your domain name and *<ip address>* is the IP address of your DNS server.

     Add more `nameserver` *<ip address>* lines as needed for each additional DNS server you want to include.
   - Press **Control-X**, then **Y** to save changes, and then press the **Enter** button to write out the file.
   - Select **`No changes`** to return to the Main Menu

The Main Menu

Once you have completed the initial setup process, the Main Menu will be your starting point for all future ThinManage Appliance modifications.



Main Menu Options: Reference Chart

Set bwadmin password	Select to enter a new password for the **bwadmin** account
Change Timezone	Select to change the server's current timezone
Change Hostname	You may change the hostname of the ThinManage server. The default hostname is set to **ws-broker**.
Enable/disable ssh server	SSH is disabled by default. You may wish to enable SSH if you plan on accessing the command line of the ThinManage server from another machine.
Reconfigure networking	Access the **Networking Menu** to: ➢ Modify Static Network settings ➢ Enable/disable DHCP ➢ Manually edit the local DNS file (`resolv.conf`) ➢ Manually edit the `/etc/network/interfaces` file.
Configure Database	The default database is SQLite. You may choose to configure the external database to use MS-SQL instead.
Restart ThinManage	**Reboot** the ThinManage server
Halt machine	**Shutdown** the entire ThinManage virtual machine.
View Server Status	Displays current status of the server and web interface.

Final Configuration Steps

DNS Configuration

On your DNS server, create an entry for **`ws-broker.<mydomain*>.<mytld*>`** that points to the IP address of the ThinManage virtual machine. This allows devices to find ThinManage automatically.

***** Where <mydomain> is your domain name and <mytld> is the top level domain. For example:

ws-broker.myXyzConsulting.com
ws-broker.HiTechSolutions.net
ws-broker.development.org

Alternative Configuration for Environments without DNS

If you don't have access to a DNS server, you can add an entry for `ws-broker` in the terminal's “hosts” file. Follow these steps on each thin client you want to manage with ThinManage:

- Login as Administrator and select **`Start Menu -> All Programs -> FBWFGUI`**
- Temporarily disable the write filter by clicking the **`Disable FBWF`** button, then press the **`Apply`** button.
- Reboot the the thin client.
- Login again as Administrator.
- Use **Notepad** to open `C:\WINDOWS\system32\drivers\etc\hosts`
- There should be at least one entry in there for localhost. Add a new line that has the ip address of your ThinManage server, followed by the name, `ws-broker`.

  For example:

  ```
  127.0.0.1          localhost
  <ThinManage-ip>    ws-broker
  ```

- Save and close the hosts file. Launch the FBWF Manager and click the **`Enable FBWF`** button. Also, make sure to re-enable the “Basic Exclusions”. For default exclusions, this would mean selecting the buttons for **`Enabled Documents and Settings for Everyone`** and the **`Enabled Persistent Registry`** buttons.
- Click the **`Apply`** button and Reboot the thin client one last time.

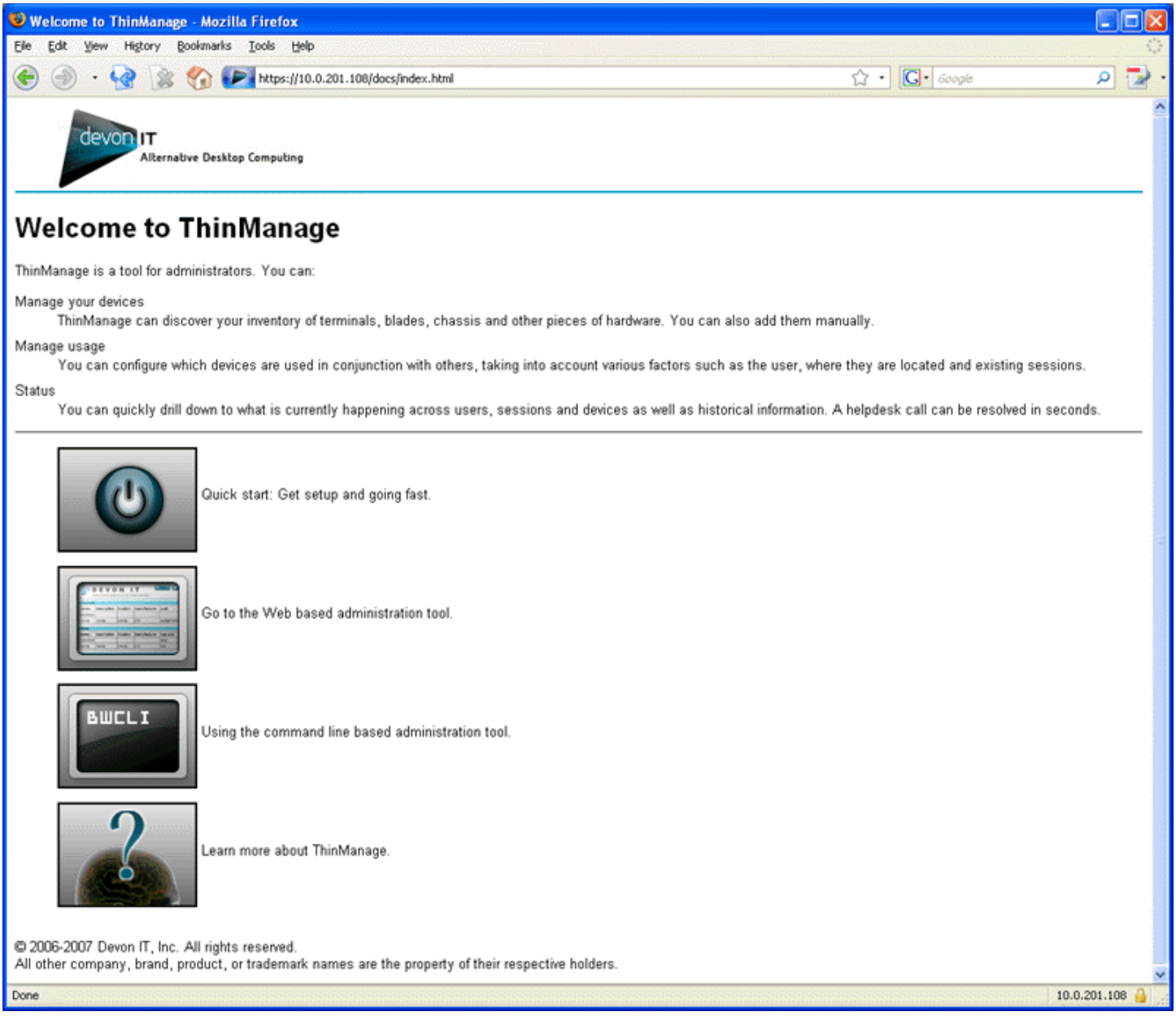
Firewall Ports

The table below describes what ports need to be open in order for ThinManage to function properly.

Port	Protocol	Component(s)	Purpose
80	TCP	ThinManage Server	HTTP – Standard web port for the ThinManage Web UI
443	TCP	ThinManage Server	HTTPS – Secure (SSL) communication over http protocol.
5500 & 5999	TCP	ThinManage Server	Needed for VNC Shadowing
50000	TCP	ThinManage Server, Hosts, and Terminals	Used by SOAP. This port needs to be open on all devices within the ThinManage environment.

Check Connectivity

Open ***http:// <Hostname or IP of your ThinManage Server>*** in a Firefox or Internet Explorer 7 web browser. If installation and setup was performed successfully, then you will be presented with the **ThinManage Welcome Page.**



Additional Installation Steps for Advanced Configurations

Please read the next two sections on this page **if you will be:**

A) Managing a Hosted Server-Desktop environment that combines HC10 / HC12 host servers with Devon IT TC10 / IBM CP20 terminals.

- OR -

B) Deploying more than one ThinManage Virtual Appliance in the same environment.

If neither of the above cases apply to your environment, then you may skip ahead to *Chapter 2, "Learning ThinManage Basics"*.

Install the Host Agent

This step is only required if you will be managing a Hosted Server-Desktop environment.

Using an administrative account, run "AgentSetup.exe" on each Host Server (HC10s or HC12s) to install the host agent. This host agent secures the Windows desktop when a user disconnects, and provides Single SignOn when using Active Directory pooling.

Configure ThinManage to use MS-SQL database

These steps must be followed if you will be using multiple ThinManage Virtual Appliance.

By default, ThinManage is configured to use a single **sqlite** database that is internal to the ThinManage virtual machine. ThinManage can also use an MS-SQL database, and must do so when more than one ThinManage virtual machine is used. For example, if you plan on deploying the *Enterprise Architecture*, to take advantage of High Availability features (*see Chapter 4, section titled "High Availability"*), then you must follow these steps:

- Visit http://www.easysoft.com/member/login.phtml to register for an Easysoft ODBC driver authorization code.
- Select `Configure Database` from the ThinManage virtual machine `Main Menu`.
- Select `Select and configure a different database` from the `Database configuration` menu.
- Select `mssql` from the `Select a database` menu.
- Select `Install Easysoft ODBC driver` from the `Easysoft ODBC installation` menu. This will launch the driver installation script.
- Press Enter to read the end user license agreement. Type `yes` at the first prompt to accept the license.
- Keep pressing Enter until you see `Running the License Application`. Choose option `[2]` from the menu.
- Enter your Name, Company Name, and email address at the appropriate prompts. You can leave the other questions blank.
- When you see `How would you like to obtain the licence?`, select option `[1]`.
- Select `[0] Exit` at the next menu.
- Hit Enter at each remaining prompt to use the default settings.
- When you return to the `mssql/ODBC configuration` menu, configure the database name, ip address, port, and username for you mssql database.
- When you are finished, choose `Keep current settings` to accept your settings and return to the `Main Menu`.
- Select `Restart ThinManage` from the `Main Menu` to activate the database connection.

Chapter 2

Learning ThinManage Basics

Topics Covered :

- *Terminology*
- *Using the ThinManage Web Interface*
- *Searches*

2.0 Learning ThinManage Basics

Terminology

You should familiarize yourself with the following list of terms, as they are used throughout this document.

Terminal

This is the device in front of the user, to which their screen, keyboard and mouse are attached. Terminals can be **thin clients**, such as the Devon IT TC5 and Safebook LVO, or **server-desktop access devices**, such as the Devon IT TC10 or IBM CP20.

Host

This is a computer providing a computing environment. An example is an HC10 Blade or HC12 server residing in the data center. Each host contains a user interface daughter card (UIDC) that handles all the audio, video, and USB streams being sent to the clients via PC-over-IP™ protocol.

Session

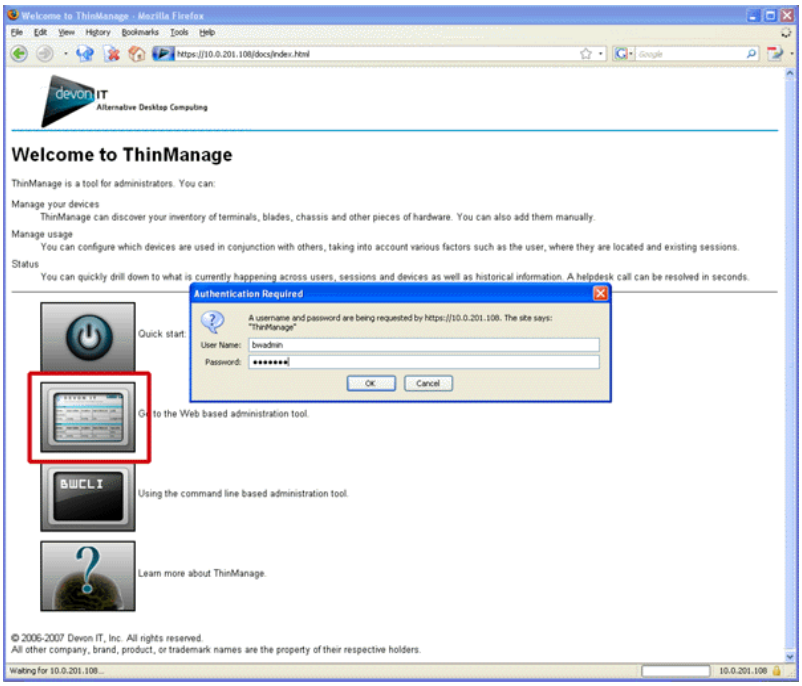
This is a network connection between a terminal and a host, with the display and USB components connected.

CMS

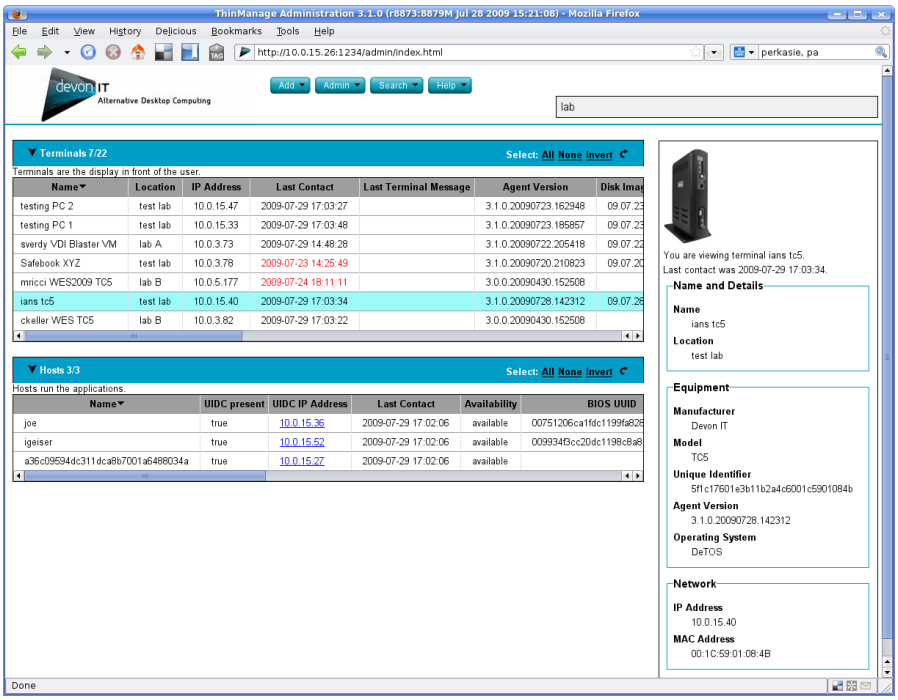
This is the connection management server, which manages connections between terminals and hosts. ThinManage is a CMS.

Accessing the ThinManage Web Based Interface

Open ***http:// <Hostname or IP of your ThinManage Server>*** in Firefox or Internet Explorer 7. Click on the image called, "**Go to the Web Based Administration Tool**" to open the ThinManage Admin GUI.



Enter **`bwadmin`** as the username and type in the password that you set during the ThinManage installation. If the ThinManage virtual machine is properly configured, and the DNS settings are correct, you will see the main **ThinManage Administration screen**.

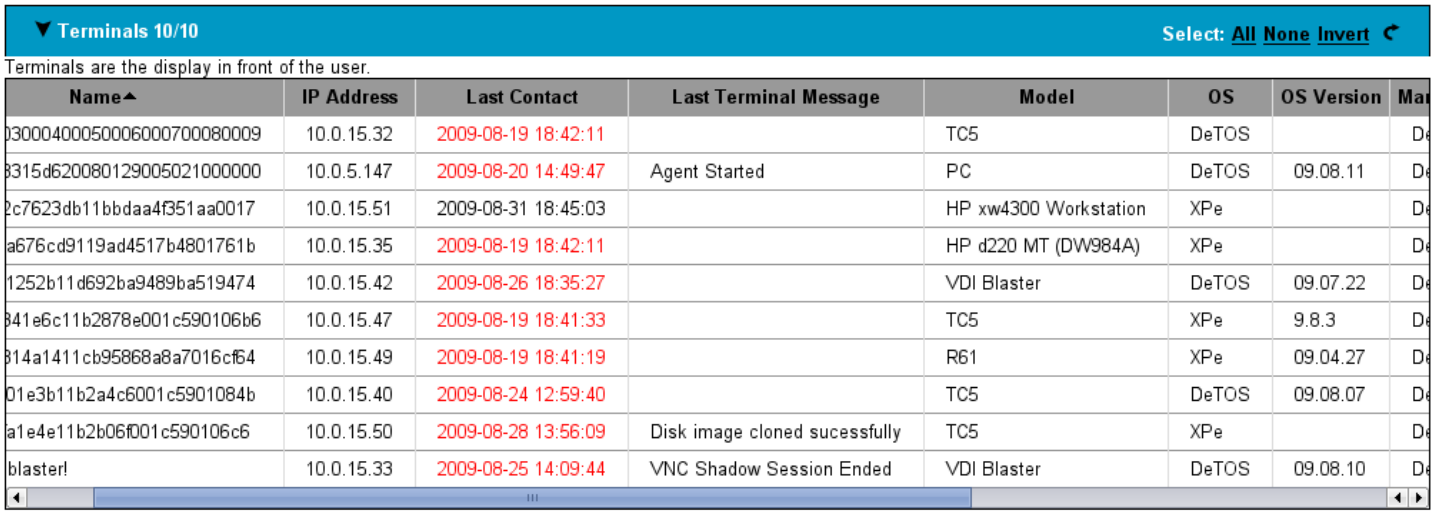


The ThinManage Administration Screen

The ThinManage Administration screen is divided into two sections. The left-hand side, spanning across approximately 75% of the screen, will display your **inventory tables** :

The "Terminals" Table

Devon IT thin clients and desktop access devices have a service called the **DeTOS Agent** that communicates back and forth with the ThinManage server. The DeTOS Agent announces its presence to the ThinManage server by continuously sending XML-based messages known as *heartbeats*. As the agent *heartbeats* into the server, information about that device will be displayed in the "Terminals" table.



Terminals 10/10 — Select: All None Invert

Terminals are the display in front of the user.

Name	IP Address	Last Contact	Last Terminal Message	Model	OS	OS Version	Ma
030004000500060007000800009	10.0.15.32	2009-08-19 18:42:11		TC5	DeTOS		De
8315d620080129005021000000	10.0.5.147	2009-08-20 14:49:47	Agent Started	PC	DeTOS	09.08.11	De
2c7623db11bbdaa4f351aa0017	10.0.15.51	2009-08-31 18:45:03		HP xw4300 Workstation	XPe		De
a676cd9119ad4517b4801761b	10.0.15.35	2009-08-19 18:42:11		HP d220 MT (DW984A)	XPe		De
1252b11d692ba9489ba519474	10.0.15.42	2009-08-26 18:35:27		VDI Blaster	DeTOS	09.07.22	De
841e6c11b2878e001c590106b6	10.0.15.47	2009-08-19 18:41:33		TC5	XPe	9.8.3	De
814a1411cb95868a8a7016cf64	10.0.15.49	2009-08-19 18:41:19		R61	XPe	09.04.27	De
01e3b11b2a4c6001c5901084b	10.0.15.40	2009-08-24 12:59:40		TC5	DeTOS	09.08.07	De
a1e4e11b2b06f001c590106c6	10.0.15.50	2009-08-28 13:56:09	Disk image cloned sucessfully	TC5	XPe		De
blaster!	10.0.15.33	2009-08-25 14:09:44	VNC Shadow Session Ended	VDI Blaster	DeTOS	09.08.10	De

The "Hosts" Table

Host servers, such as HC10's and HC12's, will have a **Host Agent** service installed. Like its DeTOS Agent counterpart, the Host Agent also communicates with the ThinManage server by *heartbeating* in periodically. When a Host Agent heartbeat is received by the ThinManage server, detailed information about that host will be reported in the "Hosts" Table*.

The "Sessions" Table

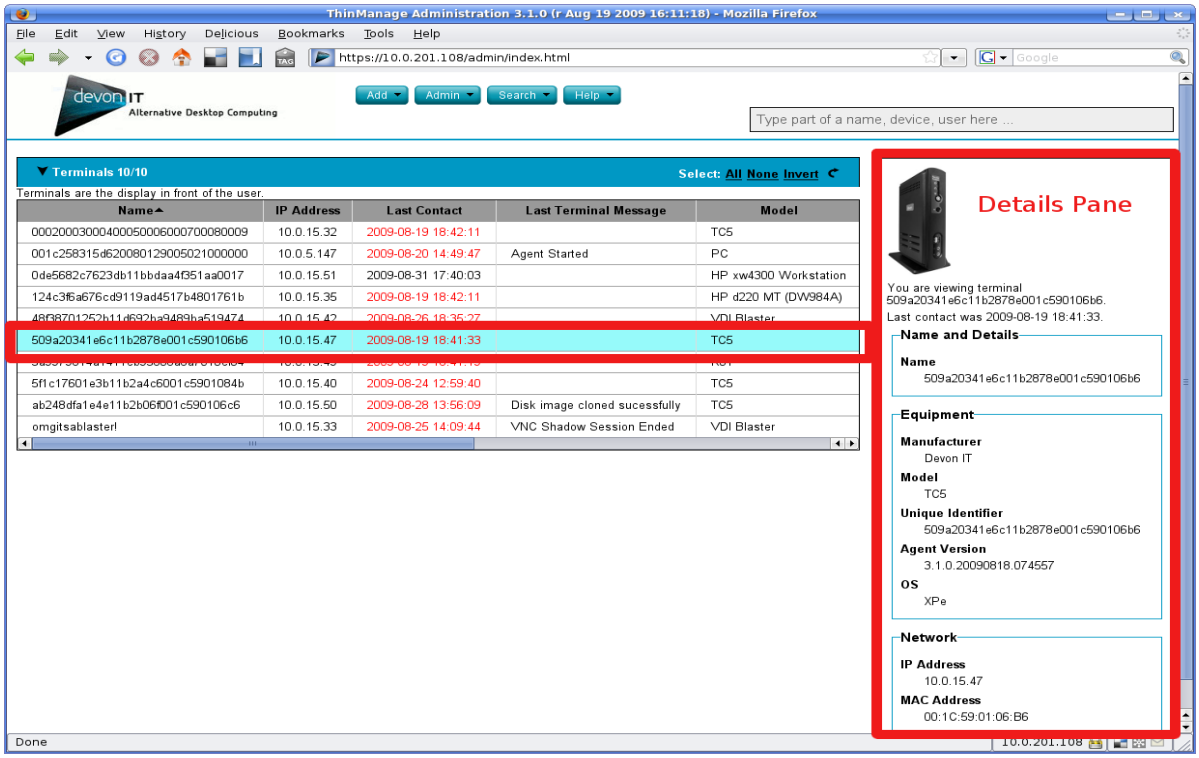
When a PC-over-IP network connection is established between a terminal and a host, details about that connection will be reported in the "Sessions" Table*.

**Note: If your environment only consists of thin client terminals, then you will only see a "Terminals" table. The "Hosts" and "Sessions" tables will not be displayed.*

The Details Pane

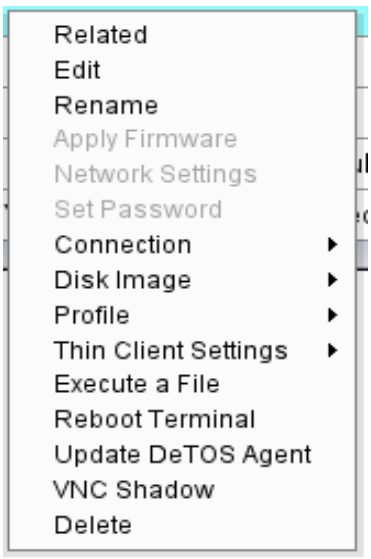
On the right-hand side of the ThinManage Administration Screen is a **details pane** that takes up the remaining 25% of the screen. Information displayed inside the details pane varies, depending on your latest mouse click event.

Left-clicking a row within a Terminal, Hosts, or Sessions table will display specific information about that object in the details pane.



The Context Menu

Right-clicking a row in any of the inventory tables will display a **context menu** with various actions that can be performed on that object. A context menu item that has an arrow beside it, indicates that sub-menu options are available for this action. Slide your mouse pointer across the arrow to access those sub-menu options.



The ThinManage Context Menu

Searches

There is a search box located near the top right-hand corner of the ThinManage Administration screen.

Simply start typing whatever you are looking for into the search box. As you begin typing each character, the items shown on the page narrow to only those that incorporate what you have typed so far. It is like using a search engine but with instant feedback.

You can type in multiple words and only items that contain all words will be shown. You can narrow down to particular fields. For example to match **`lab`**, but only in the location field, use **`location:lab`**. You should quickly be able to find whatever you want to look at.

Quoting

Place double quotes around items that contain spaces. For example **`"john smith"`**. Backslashes can also be used to escape various characters.

Attributes

To limit a match to particular attributes, use a prefix of the attribute name, followed by a colon. For example, you can type **`manufacturer:ibm`** to find all items with IBM as the manufacturer. Every item has a type. For example, to limit to results to only hosts, type **`:host`**. If you type in only the attribute name and a colon, then only items with that field and a value for it are shown. For example **`ip-address:`** will show all items that have an ip address.

Exact match

Search looks for any part of a string matching. For example if you search for lab then it will match **lab**oratory and col**lab**orate. If you want an exact match then put a plus sign in. For example **`+lab`** will only match exactly lab. It will also be case sensitive (matches are normally case insensitive).

To specify an exact match with an attribute put the **+** before the attribute such as **`+name:lab`**. If your term needs quoting then put it inside the quotes such as **`"+name:lab 20"`**.

Not

Use a minus sign to exclude items. For example to exclude any reference to John, use **`-john`**

Or

If you type multiple words then all of them must be found in an entry (conceptually there is an AND between each word). You can specify one of (or) by using OR (must be in upper case). For example john **OR** jane finds items with john or jane in them.

Grouping and complex queries

You can use parentheses around words to group them for more complex queries.
For example, **`((a b) OR -(c d)) OR e`**.

Here are some example searches:

`-description:`	Items that don't have a description
`john OR lab`	Items that have john or lab in them.
`(john OR jane OR tim) lab`	Items that have lab and at least one of john, jane or tim.
`-(john OR jane OR tim) lab`	Items that have lab, but not any of john, jane or tim.

Chapter 3

Thin Client Management

This chapter discusses ThinManage features that are specific to managing thin client devices, such as the Devon IT Safebook LVO and TC5 terminals.

Topics Covered :

- *DeTOS Agent Updates*
- *Shadowing*
- *Cloning Connections*
- *Cloning Thin Client Settings*
- *Profiles*
- *Disk Image Cloning*

3.0 Thin Client Management

DeTOS Agent Updates

The DeTOS Agent is a service that runs on the thin client devices and communicates with the ThinManage server. Periodically, Devon IT will release new Agent setup programs that provide additional functionality and/or bug fixes. The following section outlines the steps for updating a new Agent to your inventoried terminals via the ThinManage Web Interface.

Where to Download the Latest DeTOS Agent

Visit Devon IT's FTP server to download the latest DeTOS Agent installer.

FTP Location:

Server: `ftp://mx2.devonit.com`

Username: `Images`

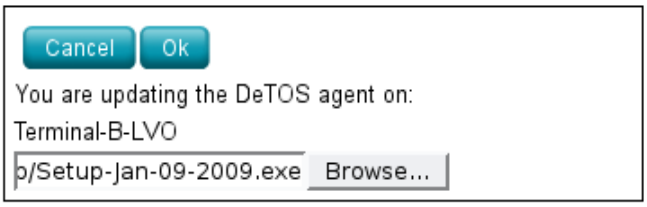
Password: `nt@t3rminal5`

Directory: ./`ThinManage/v3/DeTOS-Agent/Setup-<mm-dd-yyyy>.exe`

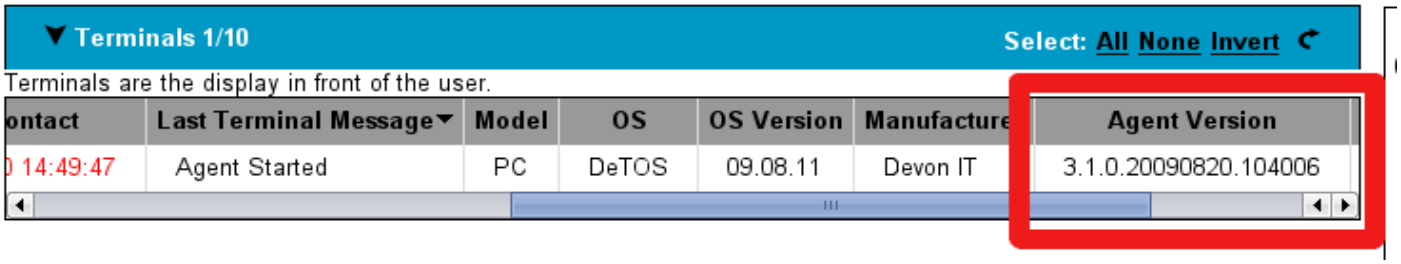
The agent installer will follow a naming convention of `Setup-<mm-dd-yyyy>.exe`, where `<mm-dd-yyyy>` will be the build date of that agent.

How to Update the DeTOS Agent on Your Terminals

1. From the table of inventoried Terminals, right-click on the terminal you want to update, and select "**Update DeTOS Agent**". To select multiple terminals, hold down the <Ctrl> key while selecting other rows, or use the <Shift> key to select a range of terminals.
2. The details pane on the right-hand side will display the terminal name(s) you are about to update. Click the **Browse** button and navigate to the new DeTOS Agent Setup executable on your local system.



3. Click the **OK** button to begin the update.
4. After a few seconds you should receive the message *"DeTOS agent request sent"*
5. The new agent will begin installing itself on the actual device. This may take 30-60 seconds. Once this installation has finished and the new agent heartbeats back to the ThinManage server, the **Agent Version** column for that terminal will display the new version number.

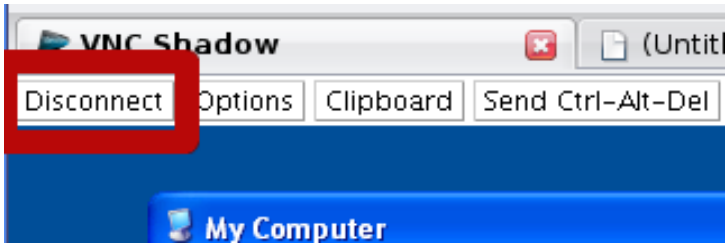


Shadowing

To help a user with their thin client, you may activate the Shadowing feature from the ThinManage Web Interface. Shadowing provides an interactive desktop session between the ThinManage administrator and terminal end-user and is an excellent tool for assisting a user with their device in real-time.

How to Shadow a Terminal

1. From the table of inventoried Terminals, right-click on the terminal you want to shadow, and select **VNC Shadow**.
2. A new browser window (or tab) will open displaying the user's screen. The cursor control is shared by both the user and administrator, so you may want to ask the user to release their mouse to avoid conflicting movements during the shadowing session.
3. When you are finished, click the “Disconnect” button located near the top of the screen to terminate your shadowing session.



Notes about Shadowing

- Please make sure your local system is using **Java Version 6 Update 11 (or higher)**. To download the latest version of Java, please visit: http://www.java.com/en/download/
- You may only shadow one terminal at a time. Initiating a new shadowing session will interrupt any active shadowing sessions you may currently have running.
- Security mechanisms are in place that only permit administrators to shadow thin clients via the ThinManage web interface. This prevents other users from simply using their own VNC client program to gain access to another user's terminal.

An Overview of ThinManage Cloning

There are three types of clones you can create with ThinManage – Connections, Thin Client Settings, and Disk Images.

Connections

Thin clients have the ability to connect to remote servers utilizing various types of protocols. The RDP protocol is used to connect to Microsoft Windows Terminal Servers. The ICA protocol is used to establish connections to Citrix servers. The VDI protocol, used by the VDM Client, allows a user to connect to a VMware VDM broker. Administrators can use ThinManage to clone these types of connections from one thin client, store them within the ThinManage database, and then apply them to other thin client terminals.

Thin Client Settings

Thin client settings are the display, sound, keyboard, mouse, and network configurations for that particular terminal. Administrators can use ThinManage to clone these settings from one thin client, store them within the ThinManage database, and then apply them to other thin client terminals.

Disk Images

The third cloning option that ThinManage offers is the ability to clone the entire disk image of a thin client terminal. A disk image includes everything that currently exists on that terminal, including the operating system itself. Disk image clones are inventoried and managed by ThinManage, but are physically stored on an NFS share or FTP server on your local area network.

The next three sections of this chapter will describe how to create and apply clones for the types mentioned above.

Cloning Connections

ThinManage allows you to clone the following thin client connections:

RDP – One or more *.rdp* configuration files used for connecting to Microsoft Terminal Servers.

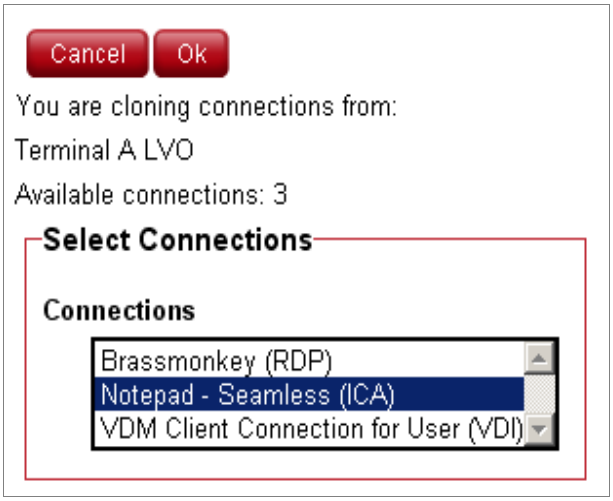
ICA – One or more *.ica* configuration files used for connecting to Citrix servers.

VDI – The User's connection settings for the VMware VDM Client.

Firefox – The local web browser and its starting URL.

How to Clone Connections

1. From the table of inventoried Terminals, right-click the terminal you want to clone, and select **`Connections -> Clone from Terminal`**.

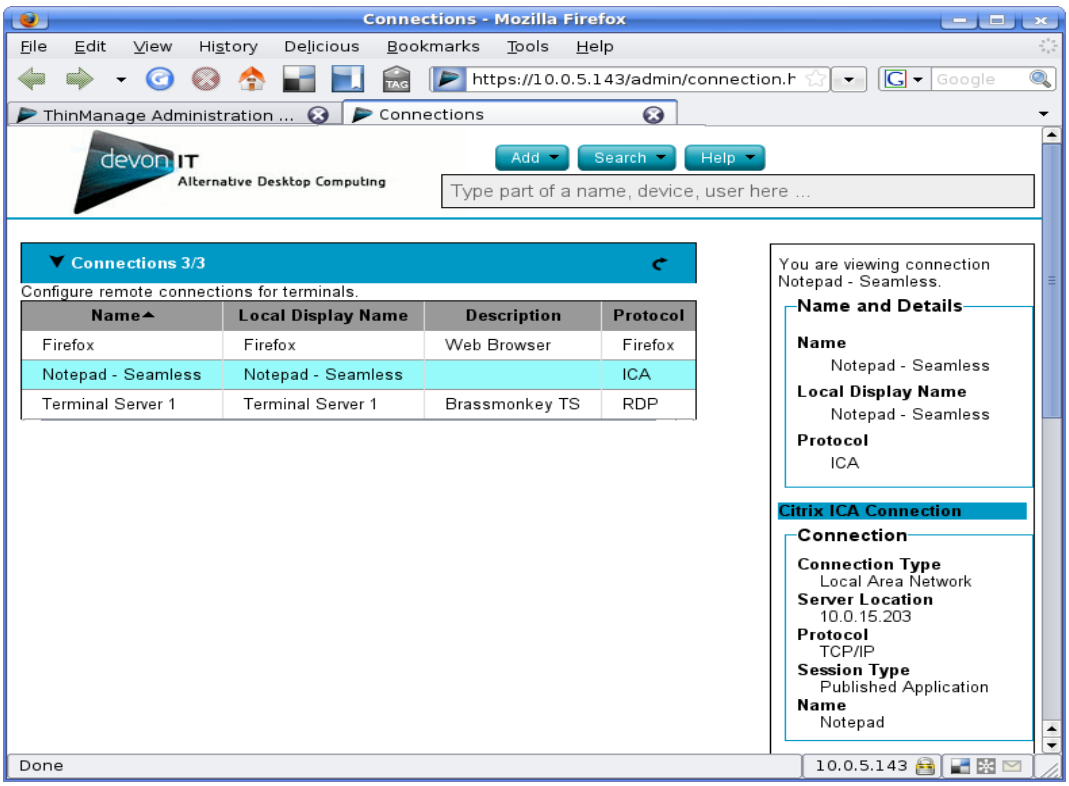


2. The details pane on the right-hand side will display the available connections you can clone from this thin client.

3. Under **Connections**, select one of the connections listed in this box. To select multiple connections, hold down the <Ctrl> key while clicking other names, or use the <Shift> key to select a range of connections.

4. Click the **OK** button. You will receive a "*Success*" message when the clone is complete.

5. From the top of the page, select **`Admin -> Connections`** to open a new screen displaying the current inventory of thin client connections. You should see your recently cloned connection entry now listed in the table.

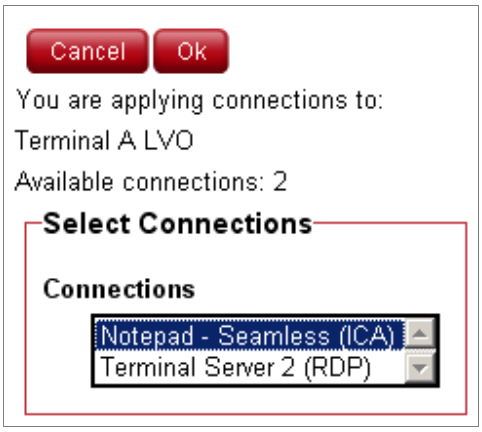


Applying Connections to a Terminal

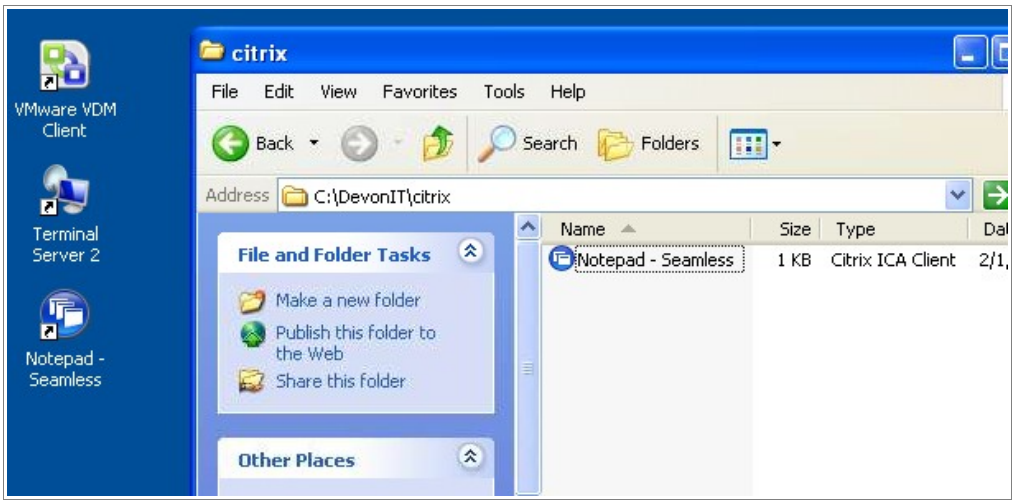
1. From the table of inventoried Terminals, right-click the terminal you want to apply settings to, and then select **`Connections -> Apply to Terminal`**.

2. In the list of **Connections**, select which connections you want to apply. To select multiple connections, hold down the <Ctrl> key while clicking other names, or use the <Shift> key to select a range of connections. You must select at least one connection – even if it is the only one available.

3. Click the **OK** button. You will receive a "*Success*" message when it is complete.



When you apply connections to thin clients, the actual ICA and RDP files are saved under `C:\DevonIT\citrix` and `C:\DevonIT\rdesktop`, respectively. Shortcuts to these files are automatically created on the User and Administrator desktops. The end user can simply double-click these shortcuts to initiate the connection.



Note About VDM Client Connections

There are a couple differences in the way VDM Client connections are handled, as compared to RDP and ICA connections. First of all, only one VDM Client connection can exist per user. Secondly, the configuration settings for a VDM Client connection are stored in the *User* account's registry hive, not in flat files like RDP and ICA. This is simply the nature of VMware's VDM Client program and not in anyway a limitation in ThinManage.

Cloning Thin Client Settings

ThinManage allows you to clone the following thin client settings:

Display – The screen resolution, color depth, and refresh rate of the primary display device.

Input – The keyboard and mouse settings.

Network – Configuration settings for the wired and wireless (when applicable) network interfaces.

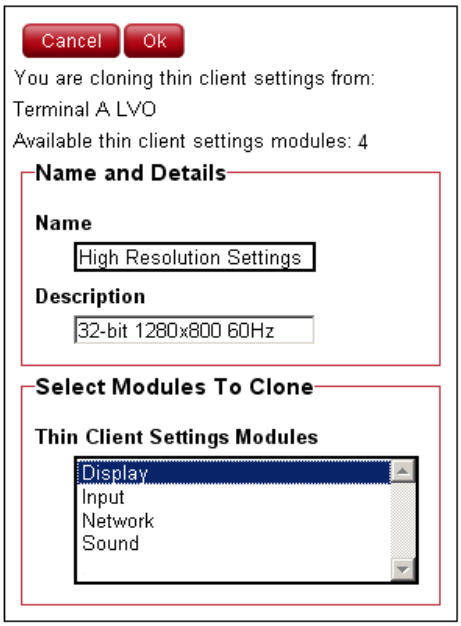
Sound – Settings for master volume and mute.

How to Clone Thin Client Settings

1. From the table of inventoried Terminals, right-click the terminal you want to clone, and select **`Thin Client Settings -> Clone from Terminal`**.

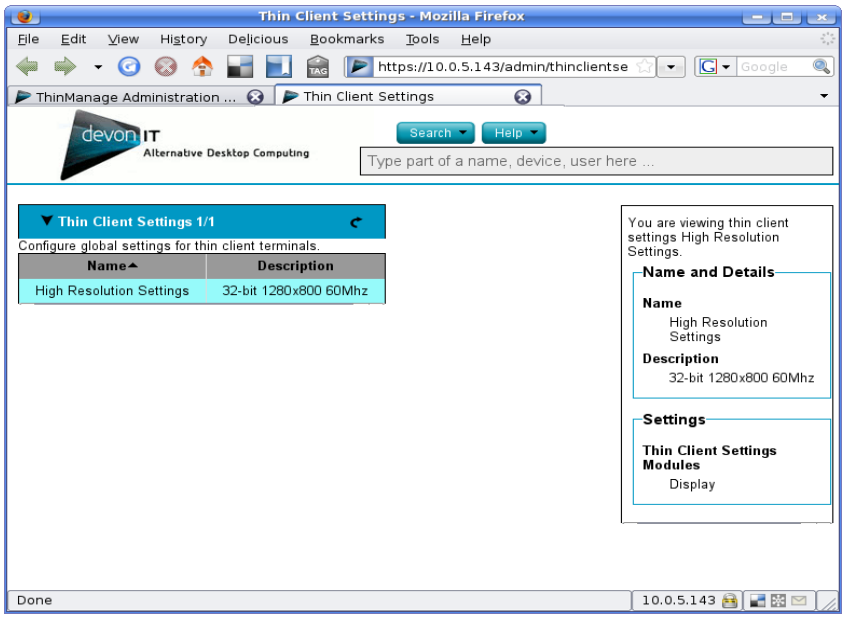
2. The details pane on the right-hand side will display a form with two sections: “Name and Details” and “Select Modules to Clone”.

   - **Name** : Enter a name for this clone.
   - **Description** : Enter a short description for this clone.
   - **Thin Client Settings Modules**: Select the type of settings you would like to clone. To select multiple modules, hold down the <Ctrl> key while clicking other module names, or use the <Shift> key to select a range of modules.



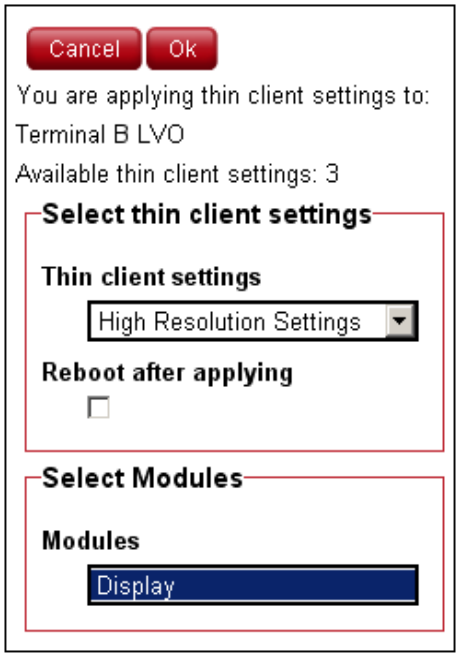
3. Click the **OK** button. After a few seconds you will receive a “*Success*” message.

4. From the top of the page, select **`Admin -> Thin Client Settings`** to open a new screen displaying the current inventory of thin client settings. You should see your recently cloned settings entry now listed in the table.



Applying Thin Client Settings to a Terminal

1. From the table of inventoried Terminals, right-click the terminal you want to apply settings to, and then select **`Thin Client Settings -> Apply to Terminal`**.
2. From the **Thin client settings** dropdown list on the details pane, select the saved settings clone you want to apply.
3. Optionally, if you would like to reboot the terminal after the settings have been applied, then mark the checkbox called **Reboot after applying**. If your new settings include network changes, then you may want to consider enabling this checkbox. Otherwise, you may leave this box unchecked.
4. In the list of **Modules**, select which settings module you want to apply. To select multiple modules, hold down the <Ctrl> key while clicking other module names, or use the <Shift> key to select a range of modules. You must select at least one module – even if it is the only one available.
5. Click the **OK** button to apply these settings to your terminal. You will receive a "Success" message once they have been applied.



Helpful Tip: If you would like to verify that your settings were properly applied to your terminal, then you may use ThinManage's Shadowing feature to gain access to the terminal's screen and inspect the system's new settings.

Profiles

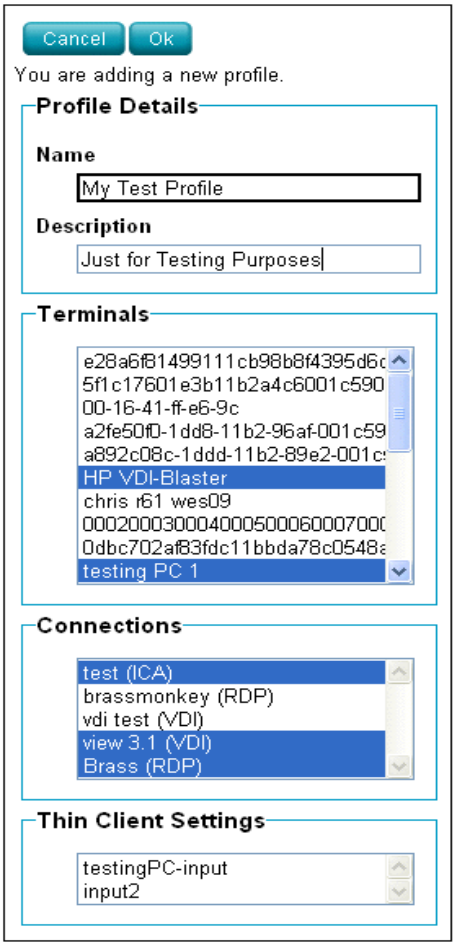
The profile feature in ThinManage allows you to assign thin client connections and settings with one or more thin client terminals. The next two sections describe the necessary steps for creating and applying ThinManage profiles.

How to Create a Profile

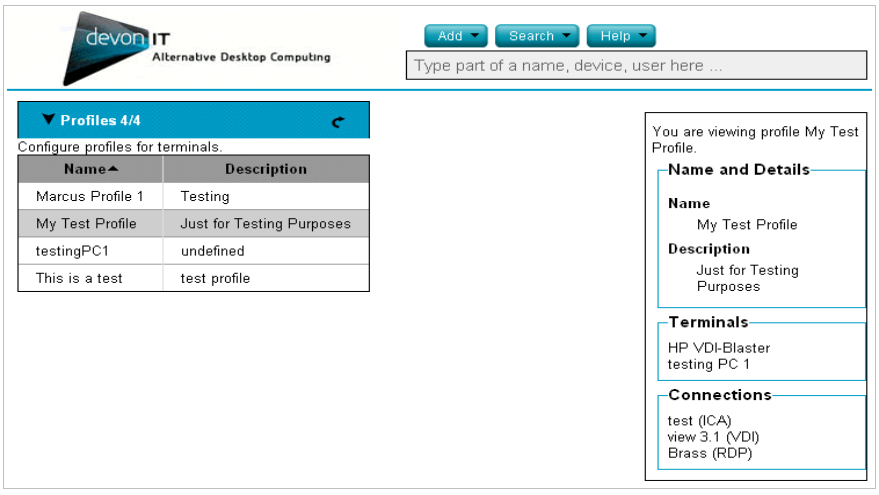
1. From the top of the page, select **`Admin -> Profiles`** to open a new screen displaying the current inventory of profiles.
2. Select **`Add -> Profile`** from the top of this page. The details pane on the right-hand side will display a "**Profile Details**" form that contains a list of 5 fields:

   - **Name** : Enter a name for this profile.
   - **Description** : Enter a short description for this profile.
   - **Terminals:** Select one or more terminals that should belong to this profile.
   - **Connections:** Assign cloned connections to this profile by selecting one or more entries* in the list. You may also choose to select none at all.
   - **Thin Client Settings**: Assign cloned settings to this profile by selecting one or more entries* in the list. You may also choose to select none at all.

   * To select multiple entries, hold down the <Ctrl> key while clicking the other entries, or use the <Shift> key to select a range of entries.



3. Click the **OK** button to create this profile. You will receive a "Success" message once it finished.
4. You should see your new profile entry now listed in the profile inventory table on the left-hand side of the screen.



Applying a Profile

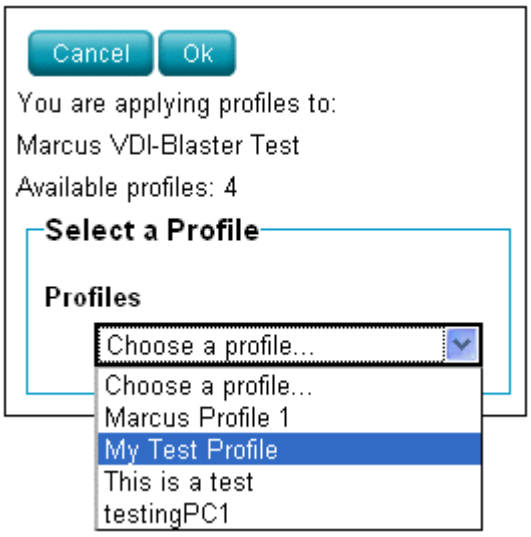
Once you finish creating a profile as described in the section above, it will automatically apply the associated connections and settings the next time the terminal is rebooted. However, if you would like the changes to take effect immediately, then you may manually apply the profile by following the steps below.

1. From the table of inventoried Terminals, right-click the terminal you want to apply settings to, and then select **`Profile -> Apply to Terminal`**.

2. From the dropdown list of **Profiles**, select which profile you want to apply.

3. Click the **OK** button. You will receive a "*Success*" message when it is finished.

4. Connection shortcuts are automatically created on the terminal's desktop. The end user can simply double-click these icons to initiate the connection.

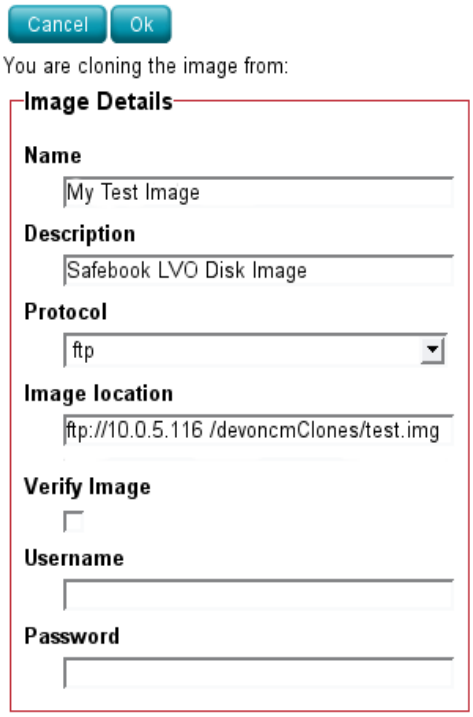


Disk Image Cloning

ThinManage allows you to perform **full disk image** cloning of your terminals, utilizing either FTP or NFS protocols.

How to Clone the Entire Disk Image

1. From the table of inventoried Terminals, right-click the terminal you want to clone, and select **`Disk Image -> Clone from Terminal`**.
2. The details pane on the right-hand side will display an "**Image Details**" form that contains a list of 7 fields:



- **Name** : Enter a name for this disk image.
- **Description** : Enter a short description for this disk image.
- **Protocol** : From the dropdown list, select either "nfs" or "ftp"
  - ***FTP*** : Select this option if you will be using an internal FTP server to store and retrieve your ThinManage disk images.
  - ***NFS*** : Select this option if you have an available NFS share on a Linux/Unix server.
- **Image Location** : Enter the protocol and location you will be using to store your disk images.

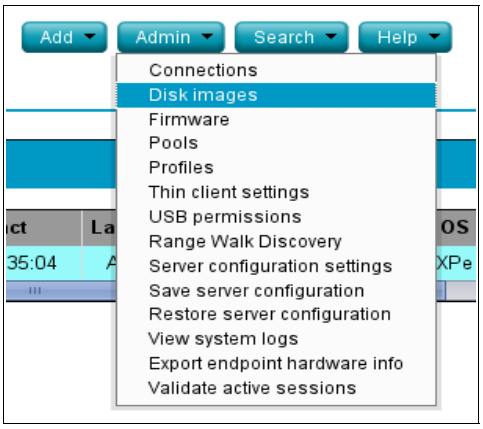
  You may use a hostname or IP address. Examples:

  `ftp://myServerName/path/to/my/image/myImageName.img`

  `nfs:/192.168.1.123/path/to/my/image/myXpeClone.img`

  *Note : The above examples use .img extensions, but you may give it any extension you want, or none at all. Also, be sure to include the protocol prefix in the url. (**ftp://** or **nfs:/**)*
- **Verify Image** : Enable this checkbox if you want perform an md5 checksum upon completion of the clone. Please be aware that the cloning process will take longer to complete when this is selected.
- **Username** : If required, enter the username of an account that has permissions to read & write to the image repository you specified in the Image Location field above.
- **Password** : If required, enter the password needed for the Username specified above.

3. Click the **OK** button to begin the cloning process. This process may take ~20-40 minutes, depending on the size of the terminal's flash disk and network traffic.
4. From the top of the page, select **`Admin -> Disk Images`** to open a new screen displaying the current inventory of disk images. You should see your recently cloned disk image now listed in the table.



Applying a Disk Image to a Terminal

Important Note: When applying disk images to your thin clients, be sure you are using the correct image for that particular model, otherwise you may render that terminal unbootable. For example, cloning a TC5 with a Safebook LVO image will not work.

1. From the table of inventoried Terminals, right-click a terminal you want to re-image, and select **`Image -> Apply to Terminal`**. To re-image more that one terminal at a time, hold down the <Ctrl> key while selecting other rows, or use the <Shift> key to select a range of terminals.
2. From the **Image Name** dropdown list on the details pane, select the image file you want to apply.
3. Click the **OK** button to begin the re-imaging process.

4. The thin client will reboot and begin re-imaging its flash media with the selected image. This re-imaging process may take ~20-40 minutes, depending on the size of the image and network traffic. During this time, there is no agent to heartbeat into the ThinManage server, and therefore the timestamp in the **Last Contact** field will remain unchanged. Once the re-image is complete and the thin client does its final reboot, the agent will heartbeat into the server, which in turn, updates the Last Contact field. This update to the current time in the Last Contact field is your cue that the re-imaging process is complete.

Devon IT Supplied Disk Images

When Devon IT releases new OS builds for its thin clients, they will be uploaded as disk images to the public FTP server. You may download these new image files, add them to your ThinManage inventory, and then re-image your thin clients using the same steps outlined in the previous section named, *"Applying a Disk Image to a Terminal"*.

Where to Download Devon IT Disk Images

Visit Devon IT's FTP server to download the latest disk images for your thin client model and operating system.

FTP Location:

Server: `ftp://mx2.devonit.com`

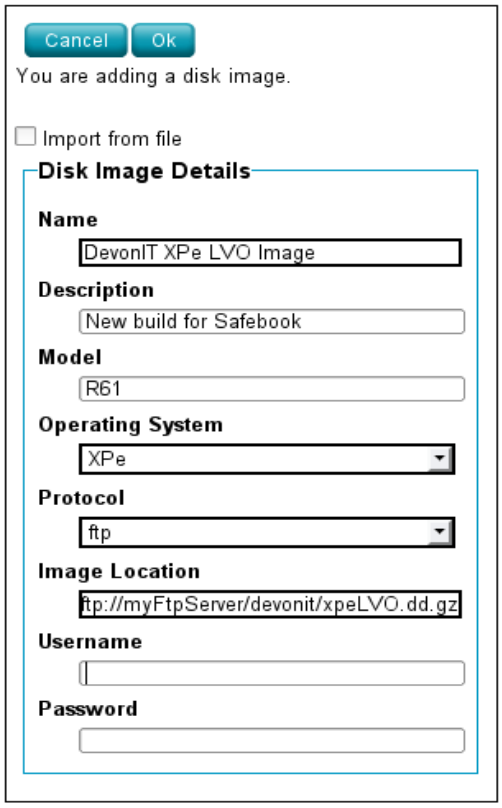
Username: `Images`

Password: `nt@t3rminal5`

Directory: `./ThinManage/v3/Disk-Images/`

How to Add a Disk Image

1. Once you have downloaded the disk image from Devon IT's FTP server, copy that image over to your FTP server or NFS shared directory.
2. From the ThinManage Administration Screen, select **`Admin -> Disk Images`** to open a new screen displaying your current inventory of disk images.
3. Select **`Add -> Disk Image`** from the top of this page. The details pane on the right-hand side will display an "**Image Details**" form that contains a list of 8 fields:



   - **Name** : Enter a name for this disk image.
   - **Description** : Enter a short description for this disk image.
   - **Model** : Enter the model name associated with this image.
   - **Operating System**: Select XPe or DeTOS
   - **Protocol** : From the dropdown list, select either "nfs" or "ftp"
     - ***FTP*** : Select this option if you will be using an internal FTP server to store and retrieve your ThinManage disk images.
     - ***NFS*** : Select this option if you have an available NFS share on a Linux/Unix server.
   - **Image Location** : Enter the location to where your Devon IT disk image resides.

     You may use a hostname or IP address. Examples:

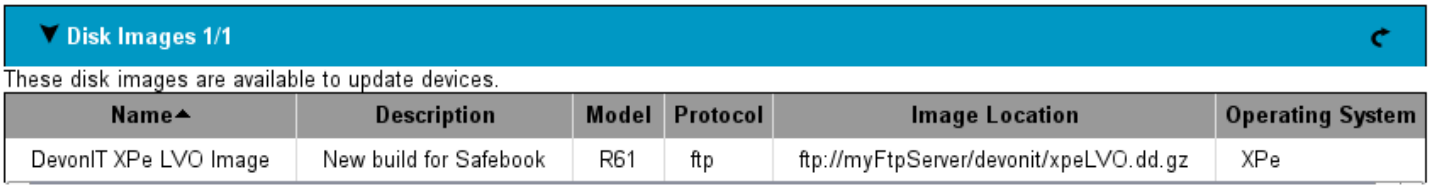
     `ftp://myServerName/path/to/my/image/<name of devonit disk image>`

     `nfs:/192.168.1.123/path/to/my/image/<name of devonit disk image>`

   - **Username** : If required, enter the username of an account that has permissions to read & write to the image repository you specified in the Image Location field above.
   - **Password** : If required, enter the password needed for the Username specified above.

4. Click the **OK** button to add this disk image.

5. You will receive a *Success* message. In the Disk Image inventory table you will now see your recently added Devon IT disk image. See section titled, *"Applying a Disk Image to a Terminal",* for instructions on how to apply the disk image to your thin clients.



Chapter 4

Hosted Server-Desktop Management

This chapter discusses ThinManage topics that are specific to managing a Hosted Server-Desktop environment that combines HC10 or HC12 host servers with TC10 / CP20 terminals.

Topics Covered :

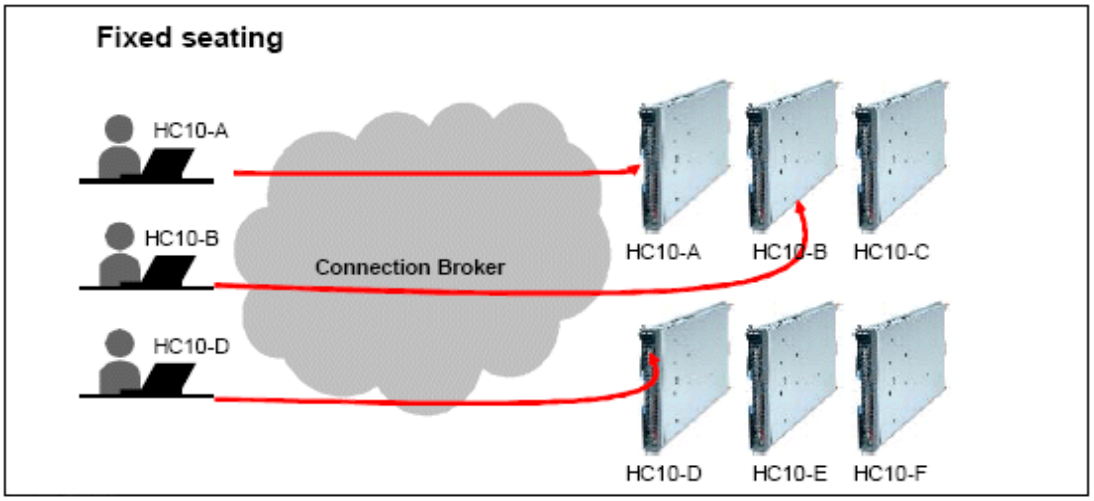
- *Connection Brokering Methods*
- *Setting up ThinManage to use Active Directory*
- *User Based Pooling*
- *Power Management and USB Controls*
- *High Availability*

4.0 Hosted Server-Desktop Management

Connection Brokering Methods

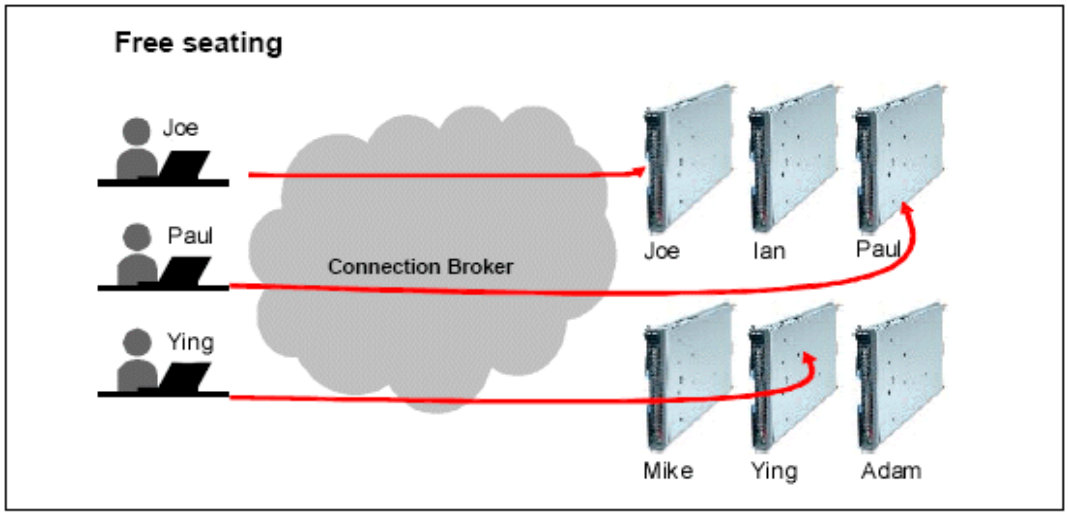
ThinManage can connect a client (user or terminal) to a Host (HC10/HC12) in three different ways:

(1) Fixed seating - Associating a **terminal** with a host. Under fixed seating, a given terminal will always connect to the same host. To configure fixed seating, rename a host device, terminal device, or both, such that their names match. It may be useful to use the MAC address of the client device as the name for both devices so that technical support personnel can easily identify the host and client devices by asking the user for the MAC address that is printed on the side of their device. Another approach is to use a name that indicates the location of the client device, such as 'cubicle A2'.



Fixed Seating Connection Method - target host is chosen based on the client device

2) Free seating - Associating a **user** with a Host. Under free seating, a user can connect to their Host from any terminal that is not already configured for fixed seating. To configure free seating, administrators need to rename a Host device to the username of the user they want to allocate the Host to. To do this in the administration tool, select the Host, right click and select *rename*, enter the new name and select OK.



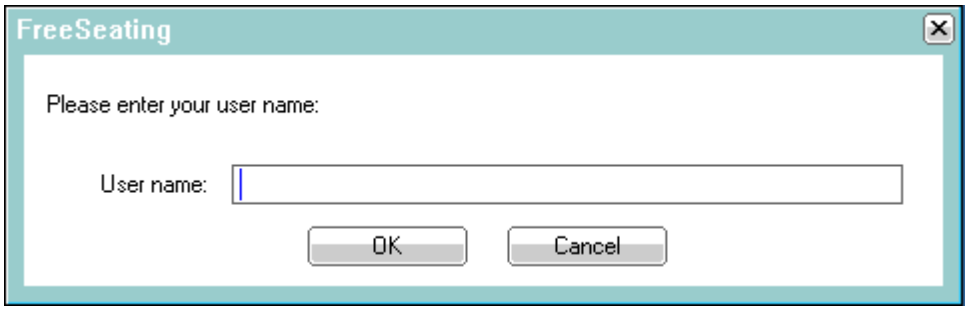
Free Seating Connection Method - target host is based on user

(3) User Pooling - Associating users with Hosts **based on Active Directory** groups. A pool is pairing of an Active Directory group of users with a group of computers. From the ThinManage web interface, click **`Admin->View/Edit pools`** to go to the pool configuration page. From there, click **`Add->Pool`** to create a new pool. Please see *Section, User Based Pooling*, for more information about the pooling connection method.

Determining the Connection Method

The names of the terminals and hosts determine the pairing method. When a terminal requests a session, ThinManage looks in its inventory for a host having the same name as that terminal. If ThinManage finds such a host, it will automatically pair the client with that host and the PC-over-IP session will begin automatically. This type of connection method is *Fixed Seating*.

Free Seating occurs when ThinManage is unable to find a host having the same name as the terminal. In this situation, the end-user will be prompted to enter a user name (see Figure below). ThinManage will now find a host matching the name provided in its inventory and proceed to connect the terminal to that host. This type of pairing can also referred to as simple named-based pairing, as no preliminary authentication by ThinManage is performed prior to establishing the connection to the host.

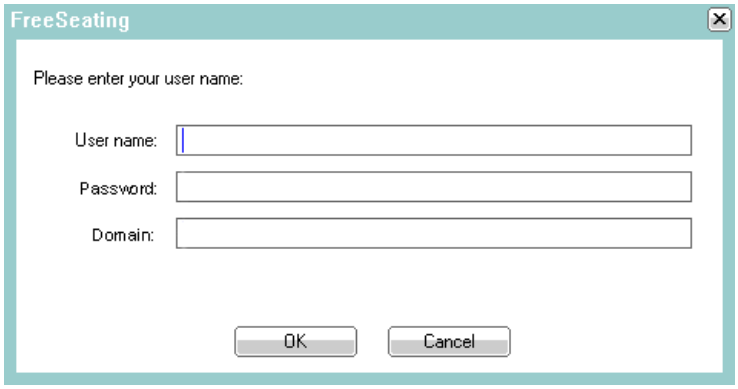


Free Seating dialog prompt that displays for Simple Named-Based Pairing

Free Seating with Enhanced Authentication

ThinManage supports a feature in the free seating connection method called *enhanced authentication*. Administrators can configure ThinManage to utilize Microsoft Active Directory to authenticate users' domain credentials before they are connected to an Host.

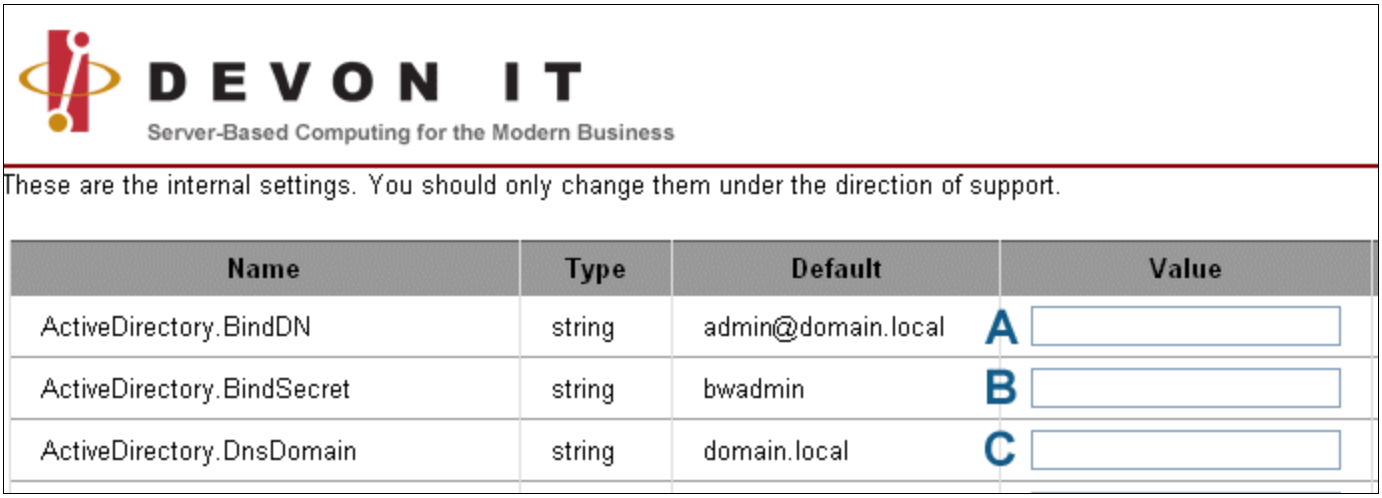
An Administrator can configure ThinManage to use AD by accessing the **Server Configuration Settings** page in the ThinManage Web Interface. Once these values are entered, enhanced authentication will be enabled within ThinManage, and an end-user will receive an extended Free Seating dialog box that now includes two additional fields for **Password** and **Domain**.



Setting up Active Directory under the Server Configuration Settings Page

From the main page of the ThinManage Web Administration Tool, select `Admin -> Server configuration settings`

This will open the internal Server Configuration Settings page for ThinManage.



Fields in the Server Configuration Settings web page that enables AD / Enhanced Authentication

There are three values that need to be entered on the Server Configuration Settings screen to connect the ThinManage server to an AD server:

A) ActiveDirectory.BindDN : This is the name of the user account that has the ability to query computer and user search DNs. An example value for this field would be: *admin@mydomain.com*

B) ActiveDirectory.BindSecret: This is the password for the user account entered above.

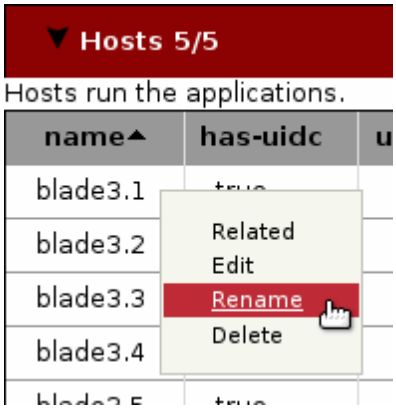
C) ActiveDirectory.DnsDomain: This is the Hostname of the AD server ThinManage will use for enhanced authentication.

How to Rename Devices with the Web Administration Tool

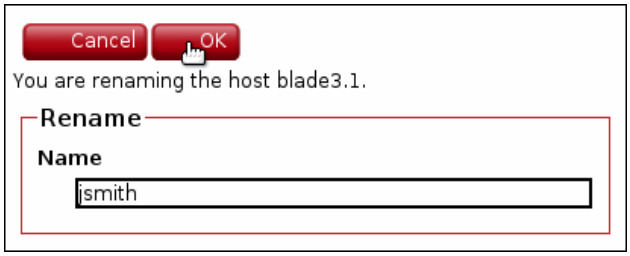
A. Open http://ws-broker.mydomain.mytld/ in Firefox or Internet Explorer 7, and click on the picture labeled 'Go to the Web based administration tool.' to go to the ThinManage administration page.

B. Rename Hosts (HC10 or HC12's):

1. Right-click a row in the 'Hosts' table, and click 'Rename'.



2. A panel labeled 'Rename' will appear on the right. Enter a new name for the host in the 'Name' field, and click 'OK'.



C. Rename terminals (TC10s / CP20s):

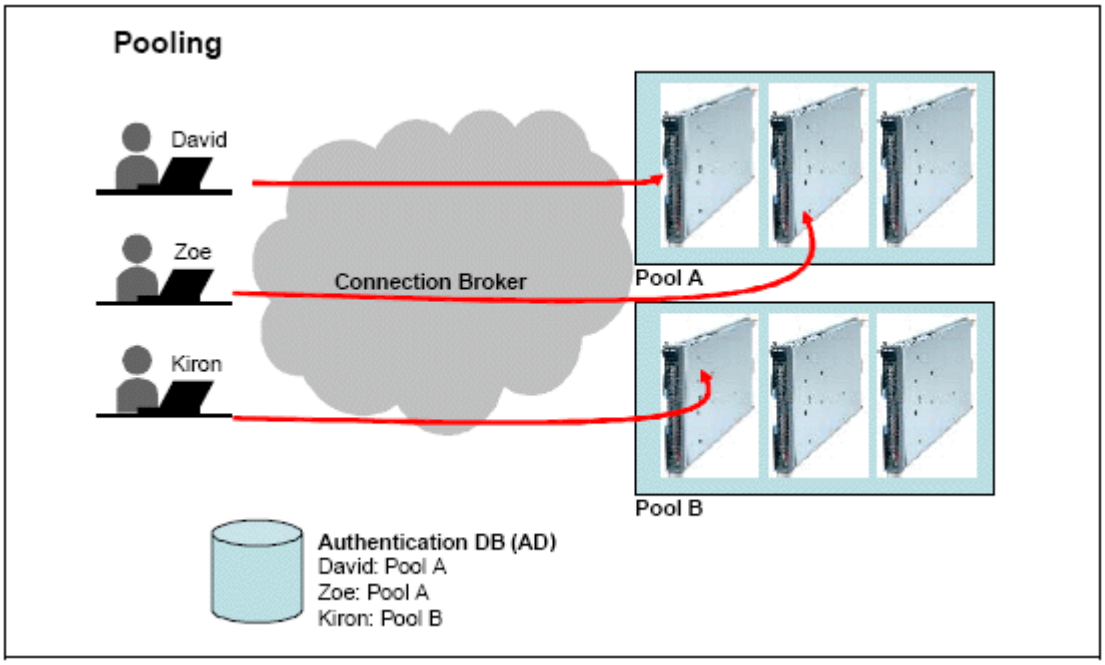
- Right-click a row in the 'Terminals' table, and click 'Rename'.
- Choose a new name for the terminal. Using the name of an existing host will establish a fixed seating pairing between the terminal and that host.
  Choosing a name that does not match the name of any host will leave the terminal in free seating mode.
- A panel labeled 'Rename' will appear on the right. Enter a new name for the terminal in the 'Name' field, and click 'OK'.

User Based Pooling

The purpose of this section is to introduce User Based Pooling and its features, describe the role that Microsoft Active Directory plays in the ThinManage pooling mechanism, and explain the rules of selection. Section 4.5 walks through a hypothetical pooling scenario to help illustrate the entire concept.

What is Pooling?

Pooling is a superset of the free seating pairing method. Instead of a user being linked to exactly one workstation Host (HC10/HC12) in the case of free seating, with pooling, that user is assigned a workstation from a pool of Hosts.[1]



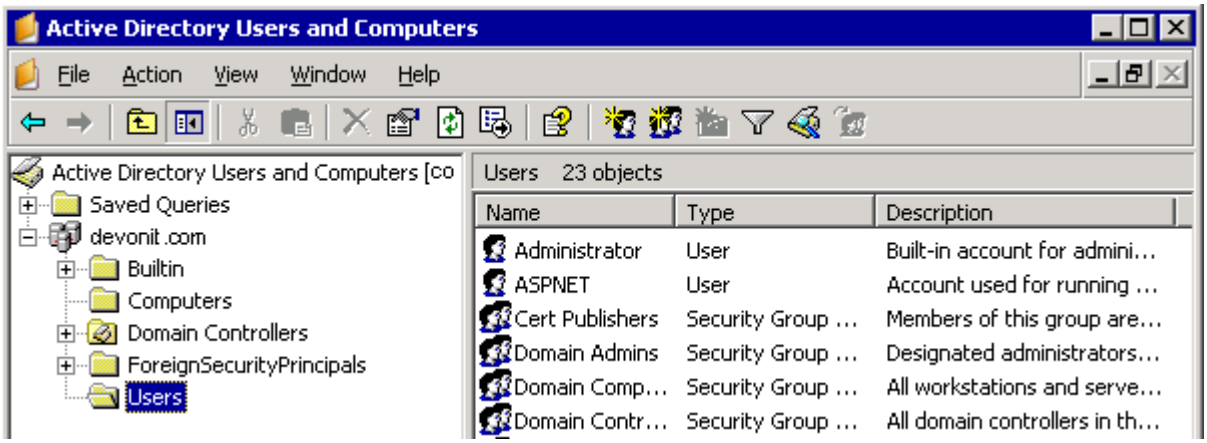
User Based Pooling Features

1. By default there is a single pool with all discovered devices.
2. Administrator can create new pools.
3. Administrator can delete existing pools.
4. Administrator can add active directory objects to an existing pool.
    e. Add user groups or objects to pool.
    f. Add machine groups or single machines to a pool.
7. Administrator can remove Active Directory objects from an existing pool.
8. Object list of acceptable objects comes from Active Directory.
    i. List Active Directory objects associated with users.
    j. List Active Directory objects associated with machines.

[1] "Implementing the IBM BladeCenter HC10 Workstation Blade," Redpaper Draft Document, September 26, 2007, IBM Corporation.

About Microsoft Active Directory

An Active Directory (AD) structure is a hierarchical framework of objects. The objects fall into three broad categories: resources, services, and users (user accounts and groups). The AD provides information on the objects, organizes the objects, controls access and sets security. Each object represents a single entity — whether a user, a computer, or a group – with each object uniquely identified by a Distinguished Name (DN).[1]



Screenshot of the "Active Directory Users and Computers" Microsoft Management Console

The benefits of using Active Directory as the datastore are twofold. First, it reduces the amount of critical information that needs to be stored inside the ThinManage server. Secondly, administrators can manage their users and hosts using normal (and familiar) infrastructure.

Creating Pools in ThinManage

Pooling in ThinManage relies on Microsoft Active Directory (AD) for its grouping information. Within their AD environment, administrators can assign users and host objects to specific groups. These groups of hosts and users are then associated by the ThinManage server to form pools.

To create a pool, administrators will use the ThinManage Web tool to associate a collection of AD users defined by a group, to a collection of AD computers (hosts) that are also defined by a group. When a users log into the system via the Desktop Access Device, they provide their username, domain, and password. This information is sent from the desktop to ThinManage over an SSL encrypted connection. By evaluating the username and domain values, ThinManage determines group membership and compares this information to the pools present. Once a pool has been identified, the Selection Rules listed below will be followed to determine exactly which Host in the pool will be assigned to that user. If no target hosts are available in the pool, then the user will receive a rejection notice, in the form of a dialog box, on the Desktop Access Device screen.

[1] Wikipedia, "Active Directory," last modified 10:18, 12 December 2007 < http://en.wikipedia.org/wiki/Active_Directory>.

An Example of ThinManage Pooling

To help illustrate the pooling concept, consider the following scenario of an administrator wanting to assign the company's developers to one group of hosts, while allocating a second group of hosts to the users working in the marketing department.

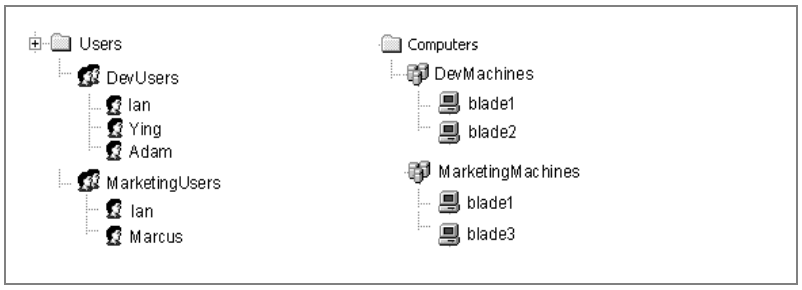


Figure 4-C: An Example AD Schema

In Figure 4-C, the administrator has created two User Groups in Active Directory. One is named DevUsers, which contains the user objects Ian, Ying, and Adam. The second group, MarketingUsers, contains the user objects Ian and Marcus. In the Computers hierarchy, the administrator has three computer objects (hosts) named blade1, blade2, and blade3 – with blade1 and blade2 associated to the DevMachines group and blade1 and blade3 associated with the MarketingMachines group.

An administrator can now use the ThinManage Web GUI to create pools based on the Active Directory schema above. (See *Section, How to a Add Pool*, for more details)

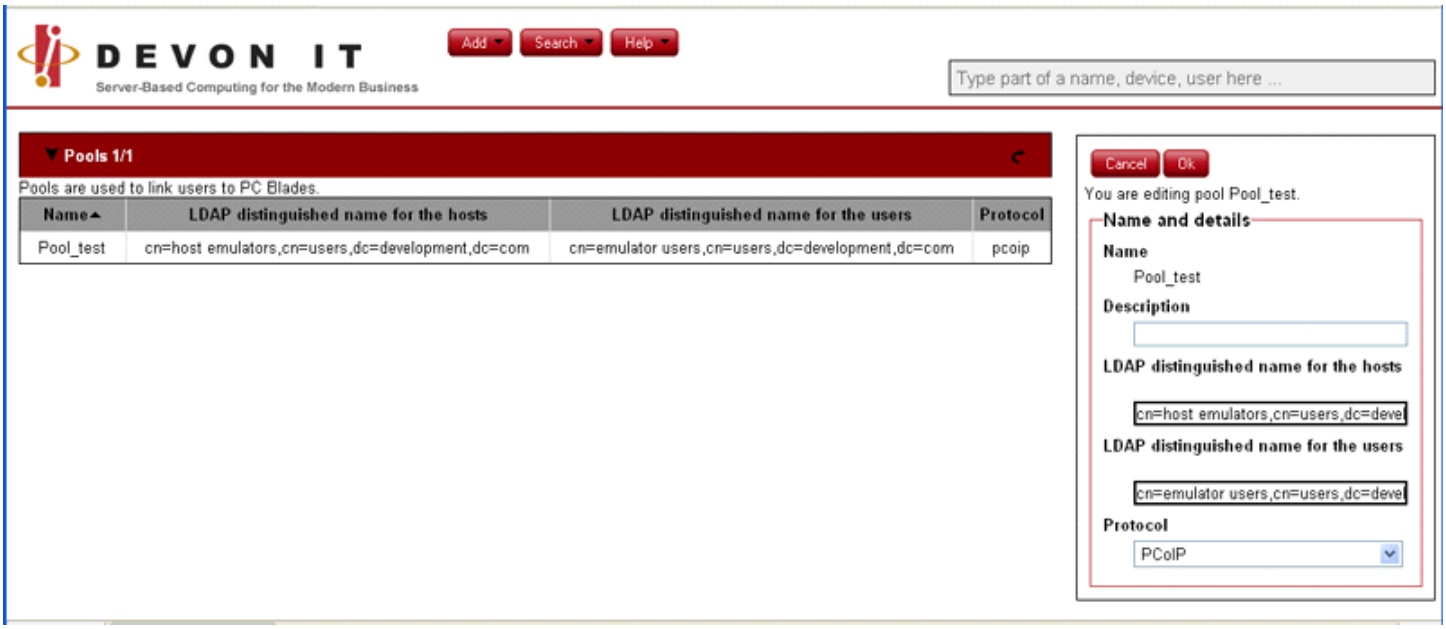


Figure 4-D: Screenshot of the ThinManage GUI for Managing User Based Pools

Now the administrator has created two pools -- "Development Department" and "Marketing Department" – effectively associating his development users with the development hosts and marketing users with marketing hosts.

Figure 4-E: Logical Associations in AD by Creating Pools in ThinManage

Now, if user Adam logs into a Desktop Access Device, he will connect to either *blade1* or *blade2*.

The user Marcus belongs to the MarketingUsers group and therefore will only ever connect to *blade1* or *blade3*. He will never access *blade2*, since that host is not a member of the MarketingMachines group.

The user Ian, being a member of both DevUsers and MarketingUsers, now has the possibility of connecting to any of the three hosts – blade1, blade2, or blade3.

Rules for Selection

In this section, the term *selection* refers the method applied by ThinManage to match a user login request with a host available at the time of the login request. Selection will choose a single item from a pool of resources. The goal of the pool will be to give out resources that have an affinity to a user. Resources will be given priorities as follows:

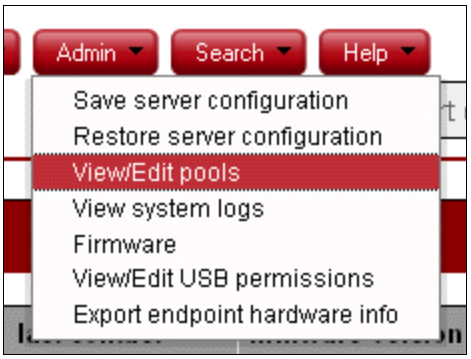
1. Check if user exists in an Active Directory group and select that pool of machine objects.
2. Select the last used host in a pool with an active windows session for the user.
3. Select the last used host in a pool with an inactive windows session.
4. Select the next free host in a pool that has had an inactive windows session the longest.

How to Add a Pool

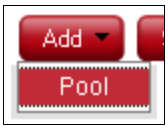
The following steps describe how to Add a new Pool, using the ThinManage Web Administration Tool.

> **Prerequisite:** Before adding any Pools, you must have Active Directory authentication enabled under the Advanced Settings page. If you haven't performed this necessary step yet, please refer to section, *Setting up Active Directory Under the Server Configuration Settings Page*, for instructions on how to do so.

- On the ThinManage Administration Interface, select `Admin -> View/Edit Pools`



- This will open a new web page used for managing your Pools.
  From the top of this page, select `Add -> Pools.`



- After selecting this option, the right-hand side panel will display the fields for adding a new pool.
  - **Name** : Name of the pool. When using the command line interface you refer to pools using their name.
  - **Description**: A human readable description of the pool, as entered by the administrator.
  - **LDAP Distinguished Name for the hosts**: The Distinguished Name of a directory service object containing a Computer or group of Computers.
    For example: *cn=devmachines,cn=users,dc=development,dc=com*
  - **LDAP Distinguished Name for the users**: The Distinguished Name of a directory service object containing a User or group of Users.
    For example*: cn=devusers,cn=users,dc=development,dc=com*
  - **Protocol**: The protocol you want used for sessions. For TC-10 terminals talking to hosts, you should use PC-over-IP (pcoip).
- Click the **OK** button to save your new pool settings. You will now see new entry for the pool you just created under the Pools table.

Power Management and USB Controls

This section describes how the ThinManage will manage the external power buttons and USB access policies on Desktop Access Devices, such as the Devon IT TC10s and IBM CP20s.

Power Management

The Desktop Access Device has two physical buttons. The top circular button on the front panel of the device is used for powering the remote HC10/HC12 Host on and off. The button located just below that is used for disconnecting an established PCoIP™ session with the remote Host. (See Figure 5-A). Power Management in this section refers to the remote power button functionality..

Figure 5-A: Desktop Access Device (TC10) Remote Power and Disconnect Buttons

Desktop Access Devices can turn off Hosts in two ways: **soft** (a single press of the power button for less than four seconds, causing the OS to be notified of a reboot) or **hard** (holding down the power button for at least four seconds, forcing an immediate reboot without informing the OS). The user is permitted to do one, both, or neither of these actions.

How To Apply Power Management Polices to Hosts

Right-click a Host entry and select “Edit”. On the right-hand side panel, there will be a section called “Access”.

There are two checkboxes called “Soft Power Permission” and “Hard Power Permission”. The description of these options are as follows:

Soft Power Permission

A boolean value that when set to true, grants permission to request a restart of the host by tapping the power button on the terminal. The host's operating system will receive the request and may or may not restart the host, depending on the operating system's power configuration.

Hard Power Permission

A boolean value that when set to true, grants permission to cut power to a host by holding down the power button on the terminal for more than 4 seconds. This request bypasses the operating system.

USB Controls

Along with modifying the behavior of the power button, an administrator also has the capability to configure which USB devices are permitted for use with a Desktop Access Device. There are options that allow all USB devices, no USB devices, or only specific USB devices. This means that if an administrator wants the users to only be able to use human interface devices (mouse, keyboard, etc), they can set the USB controls to allow this.

How To Apply USB Permissions on a Host

From the “Admin” dropdown, select the option called “View/Edit USB Permissions”. This will open a new page just for managing your USB policies. Along the top of the page will be a menu item called “USB Policy”. Select “Add Policy” from this dropdown. You will be prompted to enter a name for your policy and then click the OK button. A new entry will appear in the policy table. Clicking the entry name will open the policy settings matrix on the right-hand side panel.

The first column allows you to choose whether you would like set a policy per **ID** or per device **Class**. If you choose **ID**, then the next 2 columns in the grid must be filled in with the VendorID and DeviceID, respectively.

The other option allows you to set a policy base on the **Class** of the USB device. In this case, the 2nd and 3rd columns will be grayed out as they will not be applicable. The remaining columns are sub-class dropdown lists, allowing you to drill-down as far as you wish. If desired, repeat this process in the next row for as many type of devices you wish to apply policies for. Once you are finished, click the “save” button at the bottom left hand corner of this grid. You should receive a prompt confirming the Save action. Make a note of the policy Name you just created, as you will need to enter this in the next step.

Return to the main ThinManage Web Admin Page (where the Terminals, Hosts, and Sessions are listed). Right-click a Host for which you wish to apply your USB policy and to display the context menu. From that menu, select “Edit”. On the right-hand side panel, there will be a section called “Access”. In the USB Permission field, type in the name of the USB policy you just created. Click the OK button on the top of this panel.

From this point on, all terminals connecting to this Host will abide by the new USB Policy you just assigned to it.

A Note About Policy Application and Enforcement

While the policies for Power Management and USB Permissions are created using the ThinManage GUI, the ThinManage Server itself does not actively maintain or enforce these policies during a PCoIP™ session.

Immediately upon establishing a PCoIP™ session, event messages containing the Power and USB values are sent via Teradici’s CMI to the Desktop Access Device, informing it of the policies it should enforce. From this point on, the Desktop Access Device owns the responsibility of enforcing these rules while a PCoIP™ session is active. That fact that enforcement occurs on the endpoint, rather than the CMS, ensures that policy integrity is maintained throughout the lifespan of the PCoIP session -- even in the event of the ThinManage server going offline during the session.

High Availability

The purpose of this section is to define the concept of High Availability (HA), outline the requirements for architecting an HA-compliant system, and describe the strategies for deploying a highly available ThinManage system. This section will also present possible failure scenarios and demonstrate how the high availability aspect of ThinManage overcomes each of the hypothetical situations.

What is High Availability?

As defined by the IEEE, *High Availability* (HA for short) refers to the availability of resources in a computer system, in the wake of component failures in the system[2]. High Availability is often associated with fault-tolerant systems.

Requirements

In order to achieve an HA-compliant system, ThinManage adheres to the following requirements:

1. **Fault-Tolerant System**: ThinManage has the ability to continue service despite a hardware or software failure. Essentially, this means eliminating a single point of failure (SPOF) on the system and having failover capabilities. The result of a single component failure does not disrupt service of the entire system.

2. **Failover Capabilities**: When one component in ThinManage fails resulting in a loss of service, the service is started on another component in the system. This transfer of a service following a failure in the system is termed failover.

3. **Scalable**: ThinManage is able to support multiple concurrent connection broker servers in order to balance heavy loads.

4. **Stateless**: Each server treats each request as an independent transaction that is unrelated to any previous request on that same server or another server.

Architectures

An administrator has the option to deploy ThinManage in two different ways. The first configuration is called the *Basic Architecture*. This is a simple environment that consists of just one server, with one database repository. High availability, along with its fault-tolerant characteristics, is not present with this type of architecture.

The second option is the *Enterprise Architecture* – a three-tiered configuration that provides a more robust environment and includes all the benefits expected from an HA system. The Enterprise Architecture will be the primary focus of this section.

[2] IEEE Task Force on Cluster Computing, "High Availability (HA)" < http://www.ieeetfcc.org/high-availability.html>

The Basic Architecture – Simple and Lightweight

The Basic Architecture has one ThinManage server accessing one built-in SQLite database repository. All client requests originating from the web GUI or CLI are sent directly to a single server. The Basic Architecture is an ideal solution for an administrator setting up ThinManage in a test environment, or a small business that does not require high availability features.

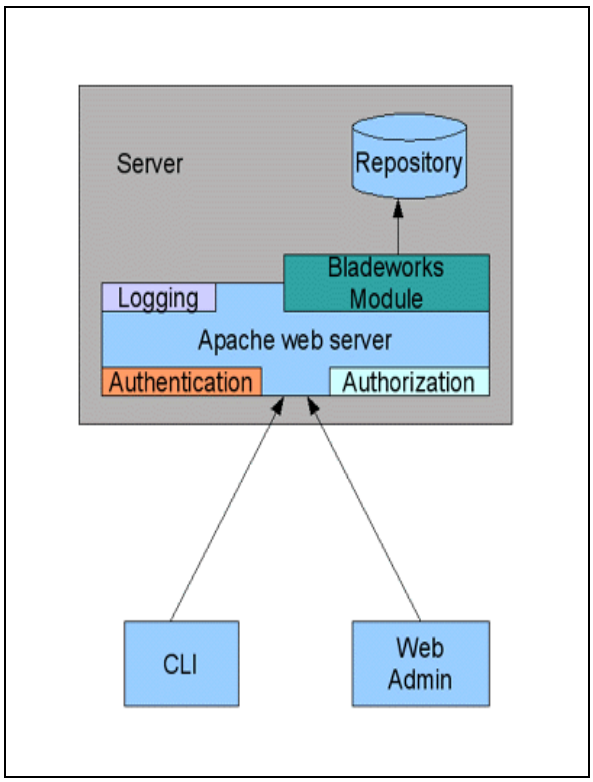


Figure 3-A : The "Basic Architecture" for ThinManage

The Enterprise Architecture-- Configuration for High Availability

The ThinManage Enterprise Architecture encompasses three distinct tiers:

- **Load Balancer**: Either a hardware or software component responsible for intelligently routing the GUI/CLI requests to one of many ThinManage servers.
- **Multiple ThinManage Servers**: The middle tier of this solution will consist of several ThinManage servers receiving requests sent via the load balancer.
- **Database Cluster**: A clustered database environment for the ThinManage servers to access shared information.

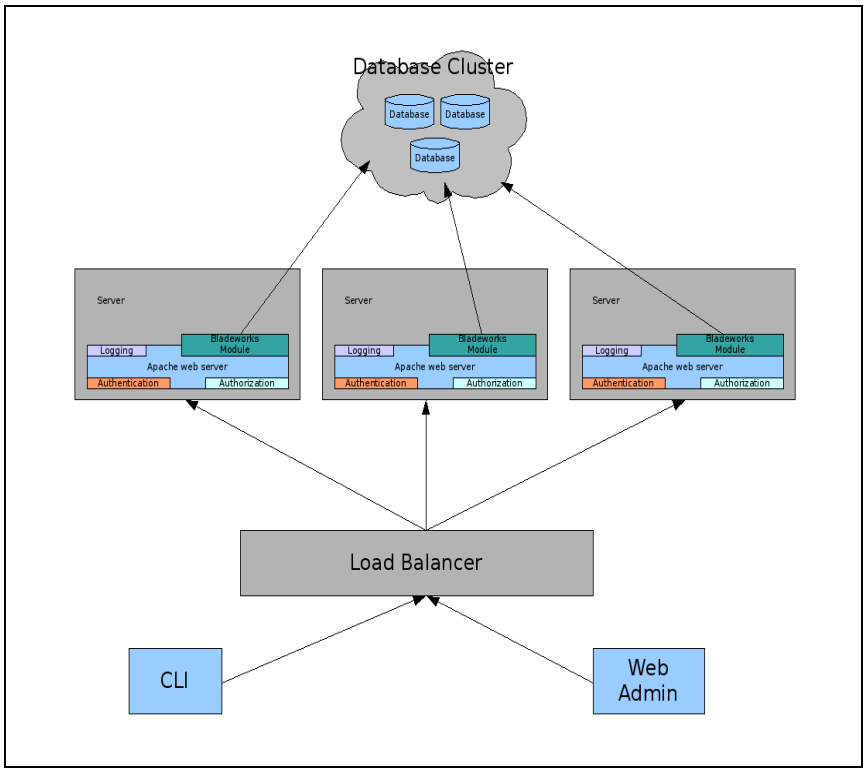


Figure 3-B : The "Enterprise Architecture" for ThinManage

All client requests originating from the web GUI or CLI are sent to a load balancer, rather than to a single ThinManage server. This load balancer, which may be hardware or software based, has the job of intelligently directing requests to one of the multiple servers available. Unlike the monolithic design of the Basic Architecture, the Enterprise Architecture does not use a single built-in database, but instead, accesses an external database cluster that is shared amongst all the ThinManage servers.

The Load Balancer

The load balancer can be implemented either as a hardware or software based solution. The next two sections describe the nature of each solution.

Software Solution for Load Balancing

One method for accomplishing load balancing would be to use a Round Robin DNS technique. Round robin works by responding to DNS requests not with a single IP address, but a list of IP addresses. The order in which IP addresses from the list are returned is the basis of the round robin name. The IP address at the top of the list is returned a set number of times before it is moved to the bottom, thus promoting the second IP address to the top of the list. This cycle is continual and allows the DNS server to assist in balancing requests between servers.[3]

Hardware Solution for Load Balancing

The second option for load balancing would be to utilize a hardware component, such as the Cisco LocalDirector appliance.

Cisco System's LocalDirector is a high-availability, Internet scalability solution that intelligently load balances TCP/IP traffic across multiple servers. Servers can be automatically and transparently placed in or out of service, and LocalDirector itself is equipped with a hot standby failover mechanism, eliminating all points of failure for the server farm.[4]

Deciding on which Load Balancing Solution to Use

The only feature a load balancer must absolutely have is the ability to redirect requests to multiple ThinManage servers. Both of the solutions presented above meet that requirement and are supported by ThinManage. Therefore, you have the choice to select which method works best for your particular environment -- and budget.

The Stateless Servers

The second tier of the Enterprise Architecture is comprised of multiple, stateless ThinManage servers. Having several concurrent servers available eliminates a single point of failure that could occur in a basic architecture that simply relies on one server for all requests. If one server goes offline - whether planned or unplanned - the load balancer can re-route requests to one of the other servers that are online.

[3] Wikipedia, “Round robin DNS,” last modified 03:40, 18 Oct 2007 < http://en.wikipedia.org/wiki/Round_robin_DNS>
[4] Cisco Systems, “Cisco LocalDirector 400 Series,” 2006 < http://www.cisco.com/warp/public/cc/pd/cxsr/400/index.shtml>.

The Database Cluster

As mentioned earlier, each ThinManage server is a stateless server. This stateless characteristic refers to the idea of a server treating each request as an independent transaction that is unrelated to any previous request on that same server or another server. Based on this notion, one may wonder how real time data can be kept in-sync throughout the entire system if each server is operating independently of one another. The answer is to have one central database that is shared amongst all the ThinManage servers.

The database management system (DBMS) to be used in the *Enterprise Architecture* is Microsoft SQL Server*.

*Note: Although the SQLite database will not be used in an Enterprise Architecture setup, it will still exist in every connection management server, as it is still needed when operating in a basic architecture environment. (see figure 3-A). A configuration setting is available in the management console to select which datastore to use. (see Section 1.7 Final Configuration Steps)

The MS-SQL DBMS utilizes database server clustering. Clustering refers to a group of two or more servers (generally called nodes) that work together and represent themselves as a single virtual server to a network. In other words, when a client connects to clustered SQL Servers, it thinks there is only a single SQL Server, not more than one. When one of the nodes fails, its responsibilities are taken over by another server in the cluster, and the end-user notices little, if any differences before, during, and after the failover.[5]

[51] SQLServerPerformance.com, "An Introduction to SQL Server Clustering," 03 April 2002 < http://www.sql-server-performance.com/articles/clustering/clustering_intro_p1.aspx>

Failure Scenarios

Now that we have outlined all the high availability features of the ThinManage Enterprise solution, we will present some possible failure scenarios that could occur and examine how ThinManage eliminates each of these points of failures.

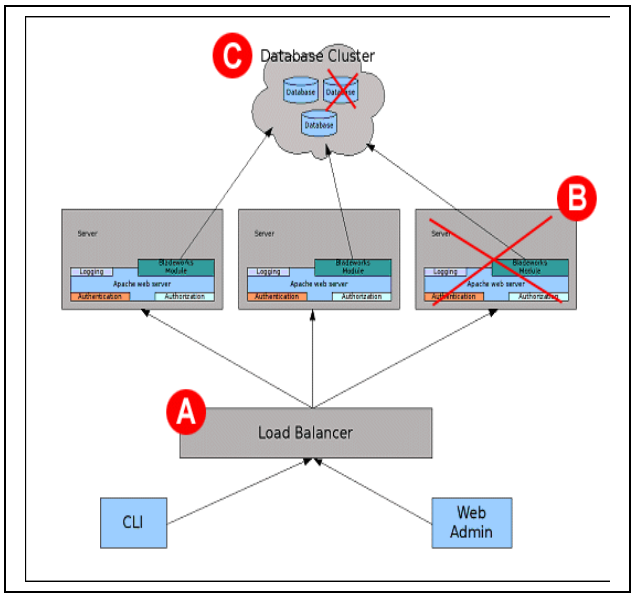


Figure 3-C: Possible points of failure in the ThinManage environment

Failure Scenario A : If a failure occurs somewhere on the load balancing tier, then requests will not be distributed to appropriate ThinManage servers. Obviously, a failure on this level would cause a breakdown of services in the system immediately. Using a load balancer equipped with a hot standby failover mechanism eliminates this possible SPOF. The Cisco LocalDirector appliance is an excellent example of a load balancing component possessing this type of failover feature.

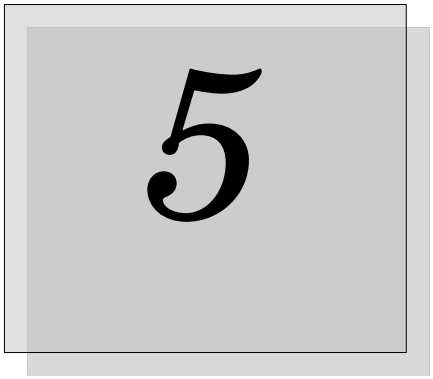
Failure Scenario B : A second component that is susceptible to failure is the ThinManage server. Generally speaking, there are two possible reasons a ThinManage server may go down:

- Planned Events: An administrator may intentionally shutdown the server for maintenance purposes.
- Unplanned Events: The ThinManage server may cease to function due to unexpected reasons, such as software glitch or accidental powering off of the host server (ie. VMware Server).

Whether the reason is planned or unplanned, the fact that other servers are online and waiting to handle new requests eliminates any possible disruption of services. The load balancer will recognize that a particular server is unavailable, and re-route the request to one of the other available servers.

Failure Scenario C: Lastly, the database itself is a potential failure point. The ThinManage servers depend on this database for retrieving scheduling and other shared information. Thus, losing connectivity to this central repository would cause serious disruption. Database clustering is the key to eliminating this situation. If one of the server nodes fails, its responsibilities are taken over by another server in the cluster.

Chapter



ThinManage Maintenance

Topics Covered :

- *Backing up your Server*
- *Server Restores*
- *ThinManage Appliance Upgrades*

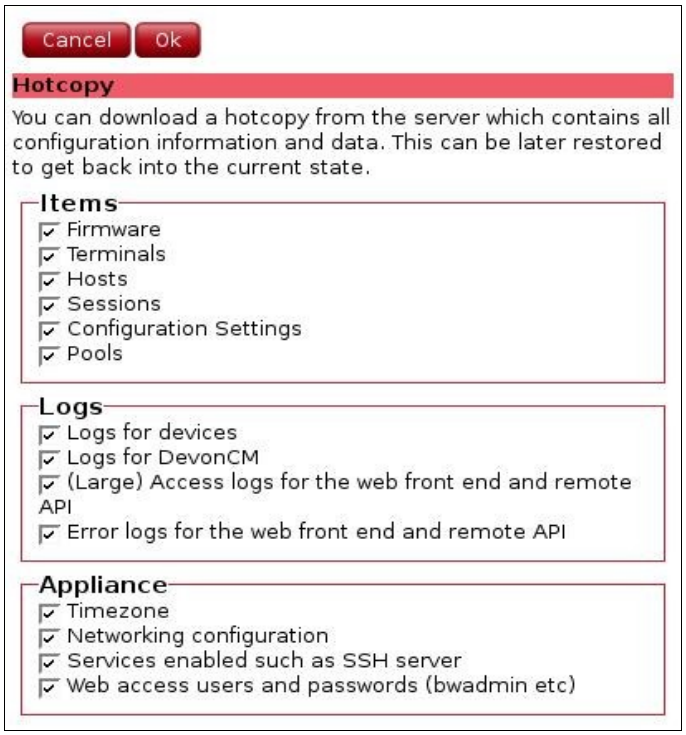
5.0 ThinManage Maintenance

Backing up your Server

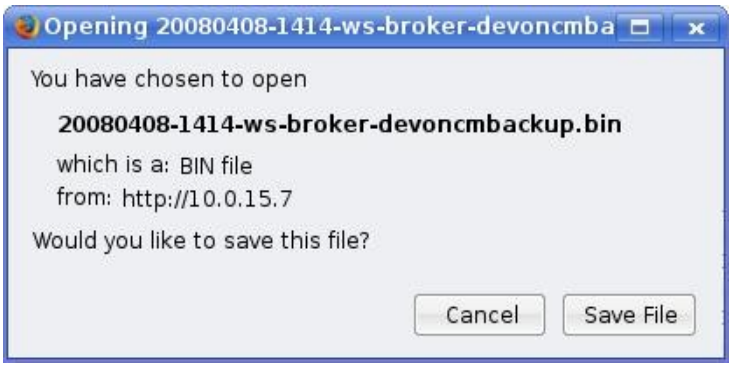
You can backup your server from the **Admin** menu. We call it **Hotcopy** since the backup happens while the system is running. There is no need to stop or suspend it for the backup. To execute a Hotcopy, do the following:

1. On the ThinManage Web Interface, select `Admin → Save Server Configuration.`

2. After selecting this option, the pane on the right-hand side of the web interface will display the `Hotcopy` informational box and will list several checkbox options, along with `OK` and `Cancel` buttons. Click **OK** to start the backup.



3. The result of the hotcopy will create a binary backup file that will be downloaded to your local machine. Make a note of where you save this file, as you will need it in the future when you perform a restore.



ThinManage Server Restore

A Restore will delete all existing configuration and data on your ThinManage Server and overwrite it with the information contained in a previously created hotcopy backup file. To perform a Restore, do the following:

1. On the ThinManage Web Interface, select `Admin → Restore Server Configuration.`

2. After selecting this option, the pane on the right-hand side of the web interface will display the `Restore` informational box. Click the **`Browse`** button to search for the Hotcopy backup file on your local machine.

3. After the path to the backup file has been entered, click the **`OK`** button to begin the Restore. Once the restore process is finished, you will receive a **`Complete`** message in the informational box.

ThinManage Appliance Upgrades

The following is the recommended procedure for upgrading your ThinManage Appliance to a newer version:

- **Step 1- Backup**: Backup your server's current configuration and data prior to performing an upgrade using the Hotcopy procedure. Refer to section *"5.1 Backing up your Server",* for details on this step.

- **Step 2- Upgrade:**
  - Shutdown the ThinManage Appliance Server (Select option 8, *"Halt machine"* from the Main Menu).
  - Download the latest ThinManage Release Trunk from http://dcmportal.devonit.com
  - Extract the contents and point your VMware Server to the new vmx file that was included in the zip archive.
  - Restart the virtual appliance.

- **Step 3- Restore:** Once the upgrade is finished and the new appliance is back online, restore your ThinManage Server. Refer to section *"5.2 ThinManage Server Restore"* for details on the restore process.